TUTTO QUELLO CHE GLI ALTRI NON DICONO

NO PUBBLICITÀ 2€
SOLO INFORMAZIONE E ARTICOLI

n.183

www.hackerjournal.it

HACKER JOURNAL

TV DIGITALE

IL REGNO DEL CAOS



eMULE

CONTROLLO REMOTO CON LINUX

HARDWARE

ARDUINO ANIMA DELLA FESTA

HACKING

CACCIA AL SISTEMA

QUATTORD. ANNO 9 - N° 183 - 23 AGOSTO/10 SETTEMBRE 2009 - € 2,00

WLF PUBLISHING

FOCUS ON

VODAFONE STATION

LIBERIAMO IL PINGUINO CHE C'È IN LEI

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



I mostri

"Invece di maledire il buio è meglio accendere una candela."
(Lao Tzu)

Alla Black Hat di Las Vegas, Joe Grand ha annunciato di aver trovato il modo di parcheggiare gratis a San Francisco: grazie a un trucchetto ha capito che basta una smart card modificata per ingannare i lettori dei parcometri. Notizia interessante se si pensa di fare un viaggio sulla west coast, certo, ma molto più interessante è il constatare che non si tratta di una notizia. Da oltre un anno, degli studenti del MIT hanno dimostrato che il trucco funziona perfettamente con tutte le macchinette mangiasoldi realizzate con la stessa tecnologia dei 23.000 parcometri di San Francisco. Se fossimo in un mondo logico sarebbero partite cause contro le società produttrici, l'obbligo di fornire apparecchi esenti dal problema e gli hacker coinvolti avrebbero avuto un encomio per averlo segnalato. Allo stato dei fatti, invece, il gruppo di studenti, che ha diligentemente segnalato il problema, è stato diffidato dal parlarne minacciando cause legali a pioggia nei loro confronti. Così, per poter divulgare la notizia, Joe Grand ha dovuto fare quello che non andrebbe mai fatto: rendere di pubblico dominio un buco in una tecnologia.

Alla luce di questo episodio diventa sinistro il futuro di Gary McKinnon, di cui parliamo nella pagina accanto, e di qualsiasi hacker "buono" che decida di segnalare la presenza di problemi di sicurezza in qualche struttura informativa. Un atteggiamento che certamente non gioverà alla creazione di sistemi di protezione e che complicherà ulteriormente la vita ai diretti responsabili: senza segnalazioni di terzi, la creazione di sistemi di protezione è un compito decisamente arduo e non permette un'immediata identificazione dei pericoli. L'ennesimo esempio di come la mancanza di collaborazione, di standard aperti, di open source possa portare a un rallentamento della tecnologia, a una fossilizzazione e a un ambiente del tutto fuori controllo e molto meno sicuro.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 9 – N.183
23 agosto/10 settembre 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Un genio in pericolo

Nel giugno del 2005, la polizia inglese, su indicazioni e su pressione dei servizi segreti americani, fece irruzione nell'appartamento di un disoccupato britannico di nome Gary McKinnon, malato di una sindrome simile all'autismo, per arrestarlo. Scordiamoci per un attimo la caccia ai terroristi e le questioni di sicurezza mondiale: Gary non era nulla di tutto questo. Era accusato di aver sferrato attacchi informatici contro i sistemi degli USA, provocando danni per un milione di dollari e violando una quantità di sistemi degni del miglior film di spionaggio: sono stati documentati 53 attacchi a reti appartenenti al circuito della difesa americana, tra cui server del Pentagono, dell'Air Force e persino della NASA. A nulla valevano i sofisticati sistemi di protezione usati dalle varie entità coinvolte: Gary era imprendibile. A tradirlo fu l'amore: sembra sia stato incastrato da una mail che ha spedito alla sua fidanzata. Il giorno del suo arresto sono cominciate le vicende politiche che lo vedono coinvolto: da una parte gli USA lo immaginano già condannato a una pena esemplare, almeno 70 anni di carcere, dall'altro la Gran Bretagna l'aveva già rilasciato in libertà condizionata perché la detenzione risulta incompatibile con la sindrome di Asperger che lo affligge. Purtroppo, gli USA sembra che, alla fine, abbiano vinto: il 9 luglio, a 4 anni dal suo arresto, il Regno Unito si è dovuto chinare alla pressione americana e lascerà che Gary venga estradato negli USA, dove già pende sulla sua testa una condanna in contumacia alla quale si aggiungeranno ben presto ulteriori processi.

Tutto questo, però, ha dato il via a una gara di solidarietà internazionale in favore di Gary e diversi esperti indipendenti hanno affermato che meriterebbe un premio e non una condanna: sotto i suoi attacchi e grazie alle falle che lui ha scoperto, i sistemi di sicurezza americani hanno guadagnato un maggior grado di efficacia, proteggendo meglio gli USA dai nemici veri. Si, perché Gary non è un terrorista, non ha violato sistemi per soldi e non ha cercato di ottenere vantaggi personali. Gary McKinnon, che ora ha 43 anni, si era semplicemente convinto che gli USA nascondessero la presenza di alieni all'interno della loro società civile e i contatti con altre civiltà spaziali e per questo motivo si mise, nel 2001, alla ricerca spasmodica di informazioni negli archivi di stato americani. Fotografie, documenti, relazioni: la sua ricerca riguardava tutto ciò che avesse a che fare con ipotesi di contatti con extraterrestri. Un motivo nobile o stupido che sia ma sicuramente un motivo che nessuna logica dovrebbe portare a una condanna "esemplare". Anche perché questa esigenza di giustizia cieca e da perseguire ad ogni costo sembrerebbe più dettata dal fatto che Gary abbia fatto fare la figura degli stupidi ai mirabili tecnici americani più che per i danni effettivamente cagionati: il milione di dollari speso per coprire i "buchi" scoperti da Gary sono ben poca cosa rispetto a quanto gli USA gli dovrebbero pagare per la sua preziosa consulenza.



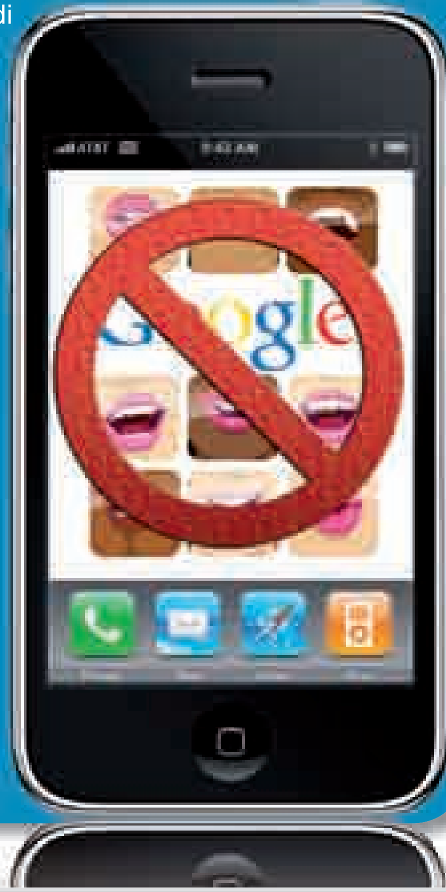
SCARICHI DA P2P? DIGIUNO!!!

Sciopero della fame contro il P2P: questa è l'insolita protesta delle aziende discografiche nigeriane e dei loro artisti per spingere il governo a varare una legge più dura contro chi scarica musica illegalmente. In Nigeria infatti, la pirateria digitale è molto diffusa e occupa i primi posti della classifica dei "reati" più praticati nel Paese Africano. Prima di arrivare allo sciopero però, i discografici, in accordo con le radio locali, hanno minacciato uno "sciopero della musica" per 24 ore che anticiperà la protesta "alimentare". Davvero un'idea originale che in qualche modo andrebbe replicata anche in Europa e negli Stati Uniti: pensate davvero che i ricchi proprietari delle major rinuncerebbero anche solo ad uno spuntino per lanciare un segnale contro chi scarica musica illegalmente? Noi non ne siamo molto convinti.



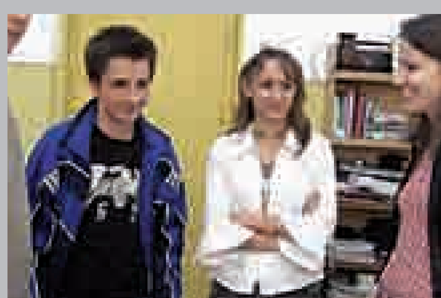
GOOGLE VOICE VIA DA IPHONE

Un'altra sconfitta per la libertà di comunicazione e un successo a favore delle compagnie telefoniche. Qualche giorno fa Apple ha rimosso l'applicazione Google Voice dal suo App Store, il "negozio" di programmi per iPhone. Ricordiamo che Google Voice è un sistema integrato che permette di comunicare a 360° con i propri contatti, utilizzando un numero di telefono "virtuale" creato da Google tramite il quale è possibile effettuare gratuitamente chiamate e inviare SMS. Purtroppo i servizi di Google Voice erano troppo in concorrenza con le compagnie telefoniche (che offrono servizi analoghi ma a pagamento) per restare su App Store. Così ancora una volta gli accordi di "cartello" tra le varie compagnie hanno troncato le gambe a un servizio gratuito che avrebbe fatto risparmiare un bel po' di soldi agli utenti di iPhone.



DA HACKER A STUDENTE MODELLO

Un libretto universitario da primo della classe con voti altissimi in matematica e fisica e una condanna per crimini informatici da scontare... studiando. Questa è la bella storia di Gabriel Bogdan Ionescu, genio romeno, arrivato nel nostro Paese come tanti e finito, come tanti, nel giro del crimine. Gabriel è un fenomeno dei computer e riesce, per pochi euro in realtà, a bucare il sistema antifrode di Poste Italiane in meno di 5 minuti, vanificando in un attimo mesi di lavoro di decine di esperti di sicurezza.



Purtroppo però le autorità scoprono la frode e Gabriel viene arrestato e condannato. Tuttavia il giudice comprende le potenzialità di questo ragazzo e, invece di mandarlo in galera con i suoi compari, lo condanna agli arresti domiciliari e a intraprendere l'università per indirizzare in modo più produttivo il suo talento. Una scelta illuminata, dal momento che oggi il 21 romeno frequenta con grande profitto il politecnico di Como: in futuro, quindi, avremo un criminale in meno sulla piazza e un esperto di sicurezza in più per difenderci dalle truffe informatiche.



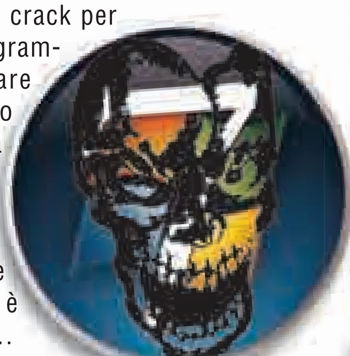
I MAC? PIÙ VULNERABILI DEI PC

Molte utenti di PC hanno recentemente deciso di fare il "grande salto" e passare a Mac. Uno dei motivi che proprio Apple adduce per preferire i suoi computer, è la maggiore sicurezza contro virus e spyware rispetto ai sistemi Windows. In realtà è esattamente il contrario: "bucare" un Mac e rubare dati sensibili è estremamente più facile che fare la stessa cosa con un PC. A dirlo è Dino Zovi, hacker italiano e vero "guru" mondiale in fatto di sicurezza informatica. Zovi infatti ha dimostrato come il kernel (il cuore) del sistema Mac OSX sia composto da un numero maggiore di stringhe di codice rispetto al suo "concorrente" Windows: chiaramente più codice esiste e più alte sono le possibilità che qualche hacker possa trovare vulnerabilità, bug e altro per accedere al sistema. Inoltre Zovi ha segnalato l'aumento di pirati specializzati in sistemi Mac OSX: una cosa da non sottovalutare dal momento che, come sostiene il nostro hacker, "finora Apple pensava che i suoi sistemi fossero protetti da una misteriosa polvere magica che ne impediva l'accesso ai pirati informatici".



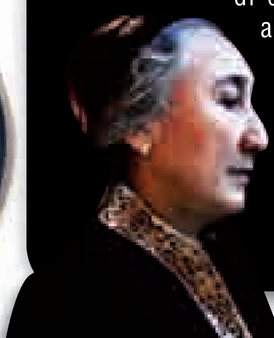
WINDOWS 7 GIÀ CRACCATO!!!

Windows 7 è già presente su molti PC in tutto il mondo nella sua versione RC: a ottobre però arriverà sugli scaffali quella definitiva al modico prezzo di 199 euro. Se state pensando di non comprarla e attendere un crack per utilizzarla senza licenza, non vi affannate: alcuni programmatori cinesi hanno infatti già provveduto a forzare l'attivazione del nuovo sistema operativo rendendolo di fatto "aperto" senza alcun tipo di restrizione. La tecnica utilizzata dagli hacker, ricalca in parte quella già usata per craccare Windows Vista. In ogni caso ci aspettiamo che, prima del suo rilascio, Microsoft trovi delle contromisure per arginare la diffusione di Windows 7 piratato. La guerra, come ogni volta, è aperta, solo che alla fine si risolverà come al solito...

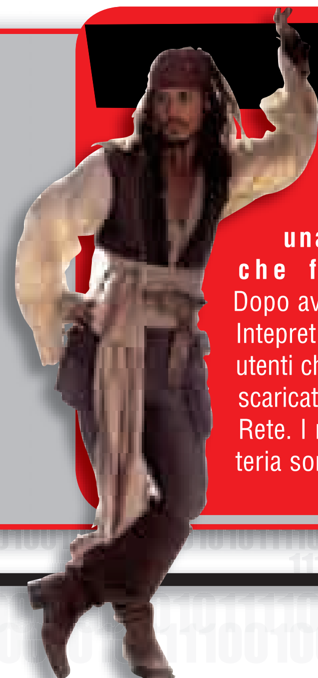


HACKER CINESI OSCURANO MELBOURNE

Il festival del cinema internazionale di Melbourne è una delle più importanti manifestazioni culturali del continente australiano. Purtroppo però quest'anno le interpretazioni degli attori, le scelte dei registi o la migliore fotografia, sono stati letteralmente oscurati dalla propaganda cinese. Alcuni hacker hanno "craccato" il sito del festival inserendo in ogni pagina la bandiera cinese e frasi contro gli Uiguri, un'etnia musulmana del Xinjiang, nel nordovest della Cina, vittima di violente repressioni da parte del governo cinese. Il festival ha avuto il "torto" di presentare un documentario che mostra gli abusi dell'esercito cinese sulla popolazione degli Uiguri, un evento che a Pechino non ha fatto piacere. A parte l'attacco informatico e l'opera di boicottaggio è triste vedere che in molte parti del mondo la libertà di espressione è ancora un traguardo lontano da raggiungere e che la Cina si muova in direzione diametralmente opposta alla tolleranza.



Su Internet oltre 24 milioni di pirati



La società di sondaggi Interpret ha recentemente condotto una ricerca sulla pirateria digitale che farà sicuramente discutere. Dopo aver intervistato oltre 64 milioni di utenti, Intepret ha concluso che sono oltre 24 milioni gli utenti che hanno, almeno una volta nella loro vita, scaricato o condiviso file protetti da copyright sulla Rete. I motivi per cui molti si dedicano alla pirateria sono sempre gli stessi: secondo gli intervistati la musica, è troppo cara, anche se alcuni sostengono di scaricare legalmente album o singoli brani da portali come iTunes che rappresentano un giusto compromesso tra prezzo e rispetto del diritto d'autore. Un dato che condanna la discografia "tradizionale" troppo cara (per il 49% degli intervistati) e per giunta qualitativamente più bassa rispetto ai nuovi formati audio in alta definizione lanciati da iTunes e soci. Dal sondaggio emerge anche un altro dato importante: se solo un terzo degli intervistati dichiara di scaricare illegalmente dal web, vuol dire che i restanti due terzi degli utenti della rete è rappresentato da inguaribili bugiardi!

COME SCIMMIOTTARE UN POLITICO

Slogan contro la destra olandese in molti siti istituzionali e foto del suo leader, Geer Wilders, opportunamente modificate per farlo sembrare una scimmia. Questo è il risultato dell'attacco hacker portato da aLpTurkTegin un hacker turco che nelle ultime settimane è diventato un vero incubo per gli amministratori di molti siti "politici" nel paese dei tulipani. L'hacker infatti, protesta contro le posizioni politiche di Wilders che si oppone all'influenza dell'Islam sulla cultura europea e all'adesione della Turchia alla Ue. Per le sue posizioni il Regno Unito gli ha vietato l'ingresso sul proprio territorio, e nei Paesi Bassi è stato denunciato più volte, ma pare che il suo partito riesca catalizzare un grande numero di elettori, che non vedono di buon occhio "l'islamizzazione" dell'Europa. Al di là delle visioni politiche, l'attacco di aLpTurkTegin rappresenta un modo incivile e poco ortodosso di protestare contro chi vorrebbe vedere il proprio Paese fuori dall'Unione.



IPHONE JAILBREAK E LA SICUREZZA NAZIONALE

In un breve comunicato rilasciato da Apple sono spiegati i motivi per cui l'azienda di Steve Jobs non approva la pratica del jailbreak, lo sblocco dei terminali in favore di applicazioni non approvate dall'App Store. I motivi "classici" ci sono tutti: instabilità di terminale e applicazioni, perdita di dati, connessioni (voce e dati) inaffidabili, molte chiamate interrotte e navigazione a singhiozzo, interruzione di servizi, come Visual Voice mail, YouTube e altri, autonomia ridotta e altro ancora. Quello che però preoccupa molto Apple, e che ci fa un po' sorridere, è la maggiore vulnerabilità del sistema operativo ad attacchi informatici che potrebbero compromettere, non i nostri documenti, i dati contenuti nei telefonini o i siti protetti che visitiamo ma addirittura la sicurezza nazionale. Insomma, una manciata di iPhone sbloccati nelle mani di terroristi o criminali, potrebbe mettere in ginocchio ogni Paese del mondo, magari provocando un altro 11 settembre. Onestamente, questa volta la società della Mela ha veramente esagerato, usando argomentazioni pretestuose e fantascientifiche per dissuadere dalla pratica del jailbreak.



QUAGLIARELLA... FURTO D'IDENTITÀ

Il giovane attaccante del Napoli e della Nazionale, Fabio Quagliarella, è stato vittima di un brutto scherzo tiratogli da una giovane hacker napoletana che è riuscita a rubare i dati di accesso al suo account di Messenger accendendovi, tra la fine del 2008 e il 2009.



Il comportamento, assai discutibile della giovane hacker, ha però insospettito i contatti del noto calciatore che lo hanno chiamato per chiedere spiegazioni. Una volta accortosi del furto d'identità Quagliarella ha subito avvertito le forze dell'ordine che in poco tempo sono riuscite a risalire alla venticinquenne napoletana autrice dello "scherzo". Uno scherzo costoso però, dal momento che adesso la ragazza dovrà rispondere davanti al giudice della sezione penale di Napoli di diversi reati che vanno dal furto di dati personali alla diffamazione: rischia il carcere e una pensante sanzione economica. Speriamo, a dire il vero, che i legali di Quagliarella considerino l'accaduto una "ragazzata" e lascino cadere le accuse.

HOT NEWS

UN BUG NEGLI SMS SPAVENTA IPHONE

Apple ha rilasciato da qualche giorno, con netto anticipo sui suoi programmi il firmare 3.01. Si tratta di una "pezza" dopo che alcuni esperti di sicurezza hanno individuato nel cellulare di Apple un bug nella gestione degli SMS che permetterebbe ai pirati di prendere il controllo del telefonino, con annesso furto dei dati sensibili in esso contenuti. Il problema tuttavia pare non essersi risolto. Infatti poche ore dopo l'uscita del nuovo firmware, altri esperti di sicurezza hanno individuato un nuovo "buco" sempre nella gestione degli SMS che potrebbe mettere nuovamente nei guai i possessori di iPhone: la sensazione è che il nuovo firmare 3.0 oltre a grandi novità, abbia portato anche ad un peggioramento della sicurezza del telefono. Insomma, occorre che Apple si prenda un po' più di tempo per elaborare un firmware che chiuda davvero tutte le porte alle intrusioni di malintenzionati: le pezze non sono mai servite più di tanto.



APPLE E GOOGLE VANNO IN GUERRA?

Eric Schmidt, CEO di Google, ha dato le dimissioni dal consiglio di amministrazione di Apple per evitare un conflitto di interessi. Non è un segreto che tra i big del mercato informatico, Google e Apple abbiano interessi che vanno lentamente a sovrapporsi: tutto ciò che Apple fa per i suoi utenti, sembra replicato, in meglio, da Google e viceversa, in una rincorsa che in origine doveva contrastare Microsoft. Rincorsa che, con tutta probabilità, vedrà nei prossimi anni una contesa tra le due aziende. Ovvio, quindi, che Jobs non volesse un infiltrato nel suo consiglio di amministrazione. In un mercato dominato da 5 aziende (le tre citate più Oracle e IBM, da anni su rotte diverse) la guerra tra le due big potrebbe portare a vantaggi inaspettati per Microsoft.

A LAS VEGAS ITALIA DOCET

Si è tenuta alla fine di luglio a Las Vegas la più importante manifestazione sulla sicurezza informatica del mondo, il Black Hat Briefings. Ogni anno nella capitale del Nevada si danno appuntamento professionisti della sicurezza delle più grandi aziende del pianeta. Grandi protagonisti di quest'anno sono stati gli italiani: Vincenzo Iozzo, studente universitario di 21 anni a Milano, già diventato leader degli hacker nostrani, ha dimostrato le numerose vulnerabilità dei sistemi Mac, iPhone compreso, e come sia possibile prendere il controllo del telefono anche con una semplice mail. Molto interessante anche la dimostrazione dei triestini Daniele Bianco e Andrea Barisano, che sono stati in grado di leggere da 50 metri di distanza quello che stava scrivendo un loro collaboratore sul suo PC semplicemente puntando un laser verso il laptop.

Black Hat

LA FIMI VUOLE LA TESTA DI PIRATE BAY

Le sventure di Pirate Bay non sembrano essere finite: nonostante i creatori del sito abbiano accettato di abbandonare la strada "pirata" per diventare un portale che vende musica e video, alcune associazioni discografiche richiedono al sito ancora dei risarcimenti milionari. È il caso anche della nostrana FIMI, l'associazione dei discografici italiani, che ha citato Pirate Bay per danni richiedendo il pagamento di 1 milione di euro a titolo di risarcimento per i file scaricati illegalmente finora. La richiesta si basa sulle evidenze raccolte nel corso del procedimento penale di Bergamo dove, sia il Giudice per le Indagini Preliminari sia il Tribunale del Riesame di Bergamo, a seguito di un'indagine della Guardia di Finanza, hanno ritenuto che Pirate Bay fosse comunque in violazione della normativa italiana sul diritto d'autore, si legge nel comunicato FIMI. Insomma, meglio tirare fuori più dobloni possibili da una nave che affonda... soprattutto se è la nave dei pirati!





La filosofia del linguaggio

Le parole spesso dicono molto di più di quello che pensiamo: impariamo ad analizzarle

Senza entrare per forza in luoghi comuni e frasi fatte, lo spunto di Reality Cracking che propongo in queste pagine è utile in moltissime situazioni della vita comune,. anche senza voler per forza tirare in ballo l'informatica. Dopotutto, Reality Cracking è anche (e soprattutto) questo: il reversing della realtà che ci circonda, che nella maggior parte del nostro tempo prescinde dall'uso del computer e che si compone in gran parte di relazioni con altre persone, con la nostra società e con il sistema che ci viene imposto.

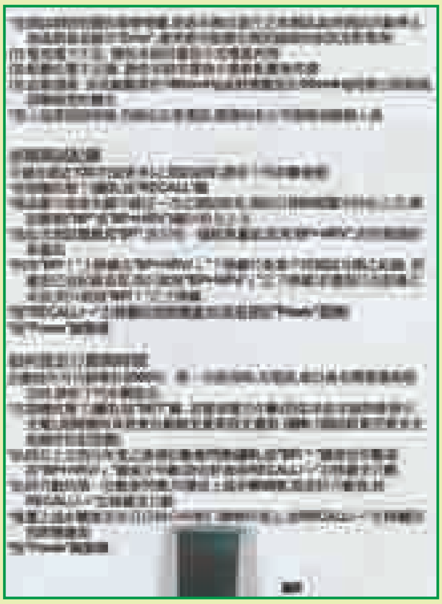
:: Studiamo le lingue!

Non è il classico consiglio della nonna o della mamma, che chissà quante volte ci hanno detto che ci serve per il nostro futuro, perché è utile per trovare un posto di lavoro e così via. Lo studio delle lingue, soprattutto della nostra, è indispensabile come autodifesa. Non possiamo pretendere di ottenere quello che vogliamo o comunque il giusto rispetto se non possiamo capire nemmeno di cosa si sta parlando, ma principalmente non possiamo proteggerci da tutti quei messaggi, scritti o parlati, che nascondono insidie o che non vogliono realmente dire quello che sembra. Studiare le lingue non vuol dire essere per forza in grado di parlarle fluentemente. Basta anche una semplice infarinatura, per così dire, uno studio superficiale della struttura della lingua, e saper tradurre un discreto numero di parole, per riuscire a capire almeno il senso del discorso. L'esempio classico è quello del libretto di istruzioni di un qualunque dispositivo: possiamo provare, se c'è, a leggere la sezione in italiano, ma nel 90% dei casi è ormai creata usando

uno dei tanti traduttori automatici presenti sul mercato e, soprattutto per tutti i gingilli prodotti in Cina, la traduzione è più simile a un monologo di Bergonzoni che a una serie di istruzioni precise e facili da capire. Con una conoscenza anche di base ma adeguata di un'altra lingua (prima fra tutte naturalmente l'inglese, ma più se ne riescono a leggere e meglio è) possiamo confrontare quella sezione con ciò che è scritto in quella italiana e colmare eventuali lacune. Io ormai leggo più frequentemente le istruzioni in inglese e a volte mi risultano più chiare di quelle in italiano, ma è solo un esempio. Se già abbiamo raggiunto un buon livello in questo primo passo verso la conoscenza del linguaggio, possiamo tranquillamente spingerci oltre e documentarci su quelle strutture, sui periodi particolari, sui costrutti gergali e dialettali propri di ogni cultura. Questa è un'arma potentissima nel mondo virtuale della Rete, dove le distanze non contano più e dove si può benissimo fingere di essere qualcun altro che risiede in tutt'altra parte del mondo. Chiunque si atteggi in questo modo nei nostri confronti, prima o poi finirà col farsi scoprire, vuoi perché compie ripetutamente un errore nella nostra lingua, vuoi perché usa modi di dire che da noi verrebbero resi in altra maniera, oppure perché ne usa certi che qui non esistono proprio. A patto, però, che noi siamo in grado di riconoscere questi segnali e di tendere una trappola adeguata nel momento in cui ci sorge il sospetto che qualcosa non vada. Parliamo di stalking. Non quello reale, l'insistenza nei confronti di una persona, l'appostamento e il pedinamento, tutte queste cose sono reato e sono perseguibili pesantemente (a ragion veduta). Lo stalking che ci serve è di quello leggero, dato dall'esperienza e dalla conoscenza soprattutto delle culture e delle lingue di altri posti del mondo. È un tipo di attacco che ci serve per risalire a chi ha effettivamente scritto qualcosa che ci è giunto per mezzo della Rete: un post polemico o comunque non adeguato in un forum, oppure una mail o un messaggio privato offensivo. Con le tecniche informatiche possiamo localizzare grossomodo da dove è partito il messaggio (locazione geografica dell'IP, traceroute verso la sorgente e così via). Lo studio del linguaggio, il confronto con altri post dello stesso utente o post simili scritti apparentemente da altri utenti in altri forum, ci potranno dare un'idea della persona che li ha scritti e potremmo trovare delle sorprese, come scoprire che diversi utenti sono la stessa persona che sta pubblicizzando o denigrando un prodotto. Provare per credere.

:: Linguaggio e psicologia

Sono le armi dei venditori di tutto il mondo e di qualunque categoria merceologica, siano batterie di pentole o aspirapolvere, siano case in multiproprietà, partecipazioni in multilevel marketing o l'appartenenza a una struttura religiosa o pseudo tale. Non ha importanza l'oggetto della transazione in sé, siamo comunque tutti a rischio quando uno di questi loschi figuri suona al campanello o semplicemente ci abborda per strada (eh sì, fanno anche questo). Saranno il suo modo di porsi, le parole che userà, gli atteggiamenti e l'insieme di tutto questo ciò da cui dovremo difenderci, ma per poterlo fare dovremo saper leggere tra le righe (ok, si parla di un discorso a voce, ma il concetto è lo stesso). Tutto ciò che deve fare questa persona è preparare il terreno, portare la vittima nel punto in cui vuole e solo allora far scattare la sua trappola. Dall'osservazione del loro comportamento, possiamo imparare da soli di cosa dobbiamo diffidare. Nella maggior parte dei casi chi vuole farci la pelle, metaforicamente parlando, sorriderà sempre, userà sempre termini positivi per esporre le proprie argomentazioni e, cosa che dovrebbe far suonare tutti i nostri campanelli d'allarme, sarà sempre d'accordo con noi, qualunque sia la nostra argomentazione. Se riusciamo a estrapolare i punti principali del suo discorso, vedremo chiaramente dove ci vuole portare. Ad esempio, piuttosto che dirci chiaramente che siamo in errore (proposizione negativa), lo sentiremo dire, estrapolando dal suo discorso, "Sì, è vero" (proposizione positiva), "anche a me una volta" (empatia: se lo consideriamo uguale a noi, saremo più inclini a credergli), "ma ho visto che" (l'alternativa), "con questo oggetto/setta religiosa/lavoro" (il contrario di quello che abbiamo detto noi). Crediamogli, e siamo fritti.



Se non conosciamo alcunché di un'altra lingua, un libretto di istruzioni che non contiene l'italiano potrebbe apparirci così.



Chi deve venderci qualcosa ha armi che difficilmente riusciremo a scoprire senza un po' di studio da parte nostra.



Informazioni carenti

L'informazione lineare parzializzata è un metodo per prendere decisioni quando l'ambito di applicazione è di tipo fuzzy

Nel 1970, un matematico polacco di nome Edward Kofler, definì quella che venne chiamata Informazione Parziale Linearizzata, abbreviata in LPI. La sua intuizione non arrivava proprio dal nulla: Kofler era professore straordinario dell'Istituto per la ricerca empirica in economia, istituito dall'Università di Zurigo, nonché uno tra i maggiori esperti al mondo di teoria dei giochi e di logica fuzzy. Il suo merito fu quello di formalizzare un concetto al limite tra matematica, filosofia, logica e scienze umane: viene chiamata Informazione Parziale Linearizzata, LPI, qualsiasi informazione parziale stocastica, indicata come SPI(p), che può essere considerata una soluzione di un sistema di disuguaglianze lineari. Questa può essere considerata come l'andamento fuzzy della probabilità p.

:: Difficile ma pratico

Il concetto è complesso quanto immediatamente applicabile all'ambito economico: basta pensare al gestore di un fondo che deve investire in azioni e al problema di massimizzare i risultati, diminuendo i rischi e cercando comunque la maggior probabilità di guadagno minimo. Proprio arrivare a definire il più alto guadagno minimo è un tema che riguarda l'Informazione Parziale Linearizzata perché non c'è alcuna equazione applicabile con certezza al problema, così come non esistono formule magiche: il funzionamento del meccanismo è totalmente calato in una logica fuzzy in cui i cambiamenti non sono predeterminabili. È facile intuire come la definizione precisa di un insieme di regole applicabili a diverse realtà e capaci di fornire risultati affidabili non sia propriamente banale. È anche vero, tuttavia, che grazie a questa teoria è possibile ricavare informazioni da scenari in cui queste sono del tutto inesistenti oppure sfuggono come tali. Una maggiore comprensione della LPI e delle sue implicazioni è possibile se si fa riferimento non tanto alla teoria di base quanto ai tre principi che ne derivano: quello di MaxEmin, quello di MaxWmin e il principio di decisione prognostica. Il principio di MaxEmin riguarda proprio l'esempio economico appena fatto: trovare una strategia capace di aumentare al massimo il minimo risultato, significa poter trovare la scelta che comporta l'impatto più positivo nello scenario. Nell'esempio economico in questione si può pensare alla scelta di titoli che potrebbero perdere valore ma non al di sotto di una certa soglia, senza considerare i titoli più redditizi: un po' co-



Sul sito blog.softwareprojects.org si parla della LPI applicata alle scienze umane in ambito lavorativo, con considerazioni sulla sua validità generale.

me chiedersi quali scelte fare per ottenere un utile nel caso peggiore. Il principio di MaxWmin è simile a quello precedente ma riguarda fattori ponderati. Riprendendo l'esempio di prima si può pensare a un investitore il cui fondo è orientato al benessere dei cittadini. Ovviamente, potrebbe essere disposto a rischiare di più sulle azioni di aziende che portano un maggior benessere generale, con un disinteresse verso quelle che considera più dannose. Così facendo, dovrebbe andare alla ricerca del MaxWmin che potrebbe non coincidere con il MaxEmin.

:: Vedo e prevedo!

La potenza della LPI, tuttavia, non sta in questi concetti ma nel terzo principio che deriva dalla sua formulazione, chiamato principio di decisione prognostica o PDP. Questo dà vita a una serie di tecniche di analisi che permettono di arrivare a prevedere, in base alla logica fuzzy, un risultato a partire da dati inesatti o incompleti. Un assunto che ha dato vita a fantasie di vario genere da parte di molti ma che ha una collocazione matematica e logica ben precisa e che, oggi, è alla base di moltissimi aspetti della nostra vita nonché principale campo di applicazione della logica fuzzy. A questo punto, tuttavia, occorre tenere ben presente che la LPI non permette di fare miracoli, così come la presenza di risultati in forma fuzzy dovrebbe dare ad intendere immediatamente che non si sta parlando di certezze di alcun genere. Fattostà che l'applicazione della LPI con la considerazione di regole chiare e l'utilizzo di dati storici certi, è la miglior strategia finora pensata per poter prendere decisioni in tempi brevi e malgrado l'assenza di informazioni complete su cui basarsi. Ovviamente occorre che questi assunti vengano rispettati e siano sottoposti a test severi prima di un'applicazione reale. Esattamente come avviene con la statistica, la correlazione di dati inconsistenti o illogici tra loro porta a conclusioni decisamente diverse da quelle che ci si può aspettare. Un problema ancora di difficile soluzione dal punto di vista informatico ma, grazie alla LPI, certamente più formalizzabile rispetto alle soluzioni basate sul semplice intuito.

EQUILIBRIO

Anche se l'informazione fornita dalla LPI è in forma di logica fuzzy, capita spesso di dover prendere decisioni frutto di strategie caute ma ottimali. Per questo motivo, il corollario più applicato della LPI riguarda quello che viene chiamato "equilibrio fuzzy": l'analisi ottenuta con l'applicazione dei tre principi di base a un intervallo temporale e di informazioni conosciuto per confermare o negare la stabilità dello scenario in cui si opera. Questo equilibrio, denominato "storico" perché valuta un punto di equilibrio sulla base di una serie di dati verificabili, è il primo passo per la ricerca dell'equilibrio del modello di LPI attuale. Questo, a sua volta, viene determinato dalla strategia più prudente necessaria per la conservazione dello stato raggiunto.

VIVA L'INTUITO?

In un certo senso, tutti noi siamo dotati di strutture mentali in grado di applicare la teoria dell'Informazione Parziale Linearizzata perché tutti agiamo sulla base di conoscenze che sono obbligatoriamente incomplete. Pensiamo, per esempio, il processo che ci porta a scegliere un'auto piuttosto che un'altra: nessuno di noi è un esperto di elettronica, di fisica, di meccanica e quant'altro sia necessario a comprendere appieno i vantaggi di un modello su un altro. Malgrado questo siamo comunque in grado di prendere una decisione fissandoci, anche inconsciamente, alcune regole sul modello che desideriamo, anche se a volte non sappiamo bene da dove derivino. Tutto il procedimento non è altro che un'applicazione empirica e informale dei principi della LPI, visti da un punto strettamente personale e non matematico. L'applicazione matematica e rigorosa, ovviamente, ci potrebbe portare a risultati diversi ma spesso incompatibili con quelli che sono i nostri normali desideri umani. È per questo che il successo nelle vendite di un'auto viene influenzato anche dalla disponibilità di colori, dalla forma dei fanali e così via...



IL CODICE SVELATO

Scoperte le chiavi di cifratura usate da Jefferson: dopo 200 anni la storia americana non ha più segreti

Il problema di proteggere messaggi, dati sensibili e corrispondenza è vecchio come il mondo. Nel periodo dell'Impero, Giulio Cesare aveva elaborato un sistema ingegnoso per cifrare comunicati e dispacci contenenti i comandi per le truppe così, nel caso in cui un messaggero fosse stato intercettato dal nemico, l'azione militare non sarebbe stata pregiudicata. Oggi esistono diversi algoritmi di crittografia con diversi livelli di sicurezza, nessuno di questi è impenetrabile. Attualmente il grado di sicurezza di un sistema di cifratura è sostanzialmente misurabile in termini puramente economici: può definirsi sicuro quando i costi da sostenere per violarlo sono più alti rispetto al valore dei dati protetti. I sistemi di sicurezza adottati dai servizi interbancari italiani, per esempio, seguono questo principio. In politica le cose sono un po' diverse. Specialmente nei periodi di grandi cambiamenti politici e sociali, la segretezza di corrispondenza e documentazione è sempre stata fondamentale per il governo di un Paese. Lo capì anche Thomas Jefferson, che in piena guerra di indipendenza inventò un sistema di crittografia per proteggere dapprima la sua corrispondenza, in seguito ogni scambio di documentazione top secret del nascente governo federale statunitense. Jefferson, insieme a John Adams, Benjamin Franklin, Robert R. Livingston e Roger Sherman ha redatto la Dichiarazione di Indipendenza degli Stati Uniti d'America, il documento che di fatto sancisce l'indipendenza delle colonie britanniche e dà il via alla nascita del nuovo Stato. Si capisce la necessità da parte del futuro terzo presidente di proteggere i suoi scritti, era fondamentale per garantire il buon esito del distacco dall'Inghil-



La lettera inviata nel 1801 da Patterson a Jefferson, in cui viene utilizzato per la prima volta il Jefferson Code.

terra. Il sistema perfetto viene inventato dall'amico matematico Robert Patterson, membro come lui della Società Filosofica Americana, che lo utilizza per cifrare una lettera spedita nel 1801, subito dopo l'elezione di Jefferson alla presidenza. Un sistema molto buono, semplice quanto ben strutturato, tant'è che ha protetto tonnellate di corrispondenza per più di duecento anni. Fino a quando, nel 2007, il dottor Lawren Smithline dell'università di Princeton ha scoperto la chiave per leggere l'incipit cifrato della dichiarazione d'indipendenza e nel luglio di quest'anno ha reso pubblica l'avvenuta decifrazione su American Scientist.

:: La forza nella semplicità

Il sistema concepito da Patterson si basava su quattro principi fondamentali: doveva poter essere applicato a tutte le lingue, doveva essere semplice da leggere e da scrivere, con un meccanismo alla base della crittografia di facile apprendimento e i messaggi codificati imperscrutabili a occhi profani. Quindi ha messo a punto quello che poi è diventato famoso come Jefferson Code, un sistema grafico basato sulla traslazione di righe e caratteri sulla base di una chiave nota alle parti. La chiave di lettura era numerica, ogni lettera del messaggio in chiaro veniva rappresentata con due cifre. La prima indicava il numero di riga e la seconda il numero di lettere da scartare partendo dall'inizio della riga. La lettera successiva all'ultima scartata faceva



Un particolare di Enigma, la macchina cifrante utilizzata dall'esercito tedesco nella Seconda Guerra Mondiale.



Il cifrario Jefferson, in una raro esemplare d'epoca. Come riferimento alla lettura veniva utilizzato il foro presente sulla parte superiore della staffa di sinistra.

parte del messaggio. Per leggere il messaggio in chiaro bisognava ordinare le lettere seguendo l'ordine esatto delle coppie di cifre dato come chiave. La prima coppia di numeri faceva riferimento alla prima lettera, la seconda coppia alla seconda lettera e così via. Dal sistema di crittografia erano esclusi i segni di punteggiatura, che non venivano considerati. Un sistema così congegnato dava due vantaggi fondamentali: l'eventuale intercettazione di una chiave, senza sapere a quale documento fosse riferita, sarebbe stata inutile; inoltre era sufficiente un testo convenzionale comune, come un libro diffuso (una bibbia per esempio) per scambiarsi messaggi cifrati senza l'invio di carteggi, col solo scambio delle chiavi di decifrazione.

:: Macchine cifranti

Successivamente il Codice Jefferson fu perfezionato con l'invenzione del Cifrario Jefferson, un cilindro composto da 36 dischi di ottone, su ognuno dei quali erano incise le 26 lettere dell'alfabeto inglese disposte in ordine casuale. Inoltre la disposizione delle lettere su ogni disco non seguiva lo stesso ordine casuale del precedente, così da avere 36 dischi diversi. Il messaggio da cifrare poteva essere composto da un massimo di 36 caratteri (tanti quanti i dischi) e la chiave di decifratura poteva essere lunga al massimo 25. Ruotando i dischi per comporre il codice di cifratura, sulla prima riga (indicata con una tacca sul supporto del cilindro) si componeva il messaggio in chiaro. In caso di messaggi più corti di 36 caratteri, veniva usata la X come riempimento. Nonostante la sua efficacia (le combinazioni di cifratura possono essere 26 elevato alla 36esima, un numero veramente enorme) entrò in funzione con potenzialità ridotte solo nel 1922 (aveva solo 25 dischi) quando fu adottato e utilizzato fino al 1950. Grande efficacia ma anche grandi limiti: mittente e destinatario del messaggio dovevano avere due cifrari identici, inoltre se un cifrario fosse caduto in mani nemiche addio sistema di sicurezza. Un cifrario analogo è apparso anche in Francia nel 1890 col dall'esercito americano nome di Cilindro di Bazeries (20 dischi), costruito probabilmente sfruttando l'idea di Jefferson che aveva lavorato proprio in Francia nei primi anni di carriera come diplomatico. Lo stesso sistema del cilindro a dischi rotanti è alla base della macchina cifrante chiamata Enigma, una sorta di macchina da scrivere utilizzata dai nazisti per proteggere i messaggi negli ultimi anni della Seconda Guerra Mondiale. Una precisazione per gli amanti del cinema di bassa lega: il Cryptex di cui si parla ne Il Codice Da Vinci e che è basato su un principio molto simile a quello del cilindro di Jefferson… è una pura invenzione letteraria, non è menzionato in nessuno scritto di Leonardo!

Spirali Psichedeliche. Arduino in festa!



Una guida alla creazione di una installazione visiva animata usando un kit Open Hardware Arduino

Tre spirali psichedeliche che si muovono a seconda della distanza dell'osservatore per creare un effetto sensoriale particolare e attraente. Un progetto divertente, di sicuro scalpore e interesse a feste e convegni!

:: Materiale di Costruzione

Nastro isolante, saldatore, pistola per colla a caldo, cartone. Le spirali psichedeliche possono essere scaricate e stampate da questo indirizzo http://blackman.amicofigo.org/gallery/v/Arduino/SpiraliPsichedeliche/ oppure scelte a piacere.

Questo progetto è nato con l'idea di stupire e incuriosire chi vi passa accanto. Si tratta di tre spirali di cartone che vengono fatte girare più o meno velocemente a seconda della distanza dell'osservatore dal sensore sonar. Ad esempio è possibile impostare il movimento in modo decrescente in un range di 3 metri una spirale che inizi a ruotare tra 3 e 2 metri, un'altra tra 2 e 1 e l'ultima quando l'osservatore è molto vicino. Le spirali variano la loro accelerazione mano a mano che ci avviciniamo al sensore. Benché la costruzione sia piuttosto semplice l'effetto ottico è davvero interessante: vale davvero la pena di provare.

MATERIALE NECESSARIO

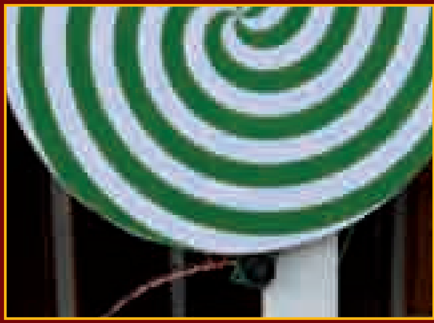
- 1x Arduino (il progetto è stato testato con Diecimila e 2009);
- 1x motor shield di Ladyada (www.adafruit.com 19.50 $);
- 1x sonar SRF02 (www.robot-italy.com 16.40 €);
- 2x resistenze di pullup. 3.3KOhm;
- 3x motori DC da 5V, ottenibili da materiale di recupero;
- 3x spirali psichedeliche da preparare stampandole e incollandole su cartoncino leggero;
- 1x stecca di pin maschi;
- 1x stecca di pin femmine;
- 2x socket per chip da 16 pin;
- 1x supporto per montare motori e girandole come un'asse di legno lunga di 2 metri e larga pochi cm;
- 2x alimentatori DC. Si consiglia un alimentatore da 5V e 2A per il motor shield e uno da 7,5V e 12A per Arduino: possiamo recuperarli da parti hardware dismesse.

:: Mettiamoci al lavoro!

Per prima cosa assembliamo, se non lo abbiamo già fatto, il Motor Shield di Ladyada. Il Motor Shield è un ottimo strumento per sperimentare i motori, è in grado di pilotare, a seconda della configurazione, fino a quattro motori dc, due motori stepper e due motori servo.
Lo shield arriva come kit di montaggio e va costruito seguendo scrupolosamente le istruzioni presenti sul sito di Ada. Il mio consiglio è quello di apportare un paio di piccole modifiche al progetto originale. Assembliamo i driver L293DNE dei motori (i chip che piloteranno i motori) su zoccoli non forniti nel kit. Questo aiuta in fase di debug, inoltre, nel caso in cui rompessimo il chip per surriscaldamento (per via di qualche motore troppo desideroso di corrente) potremo cambiarlo agevolmente. Vanno saldati sul Motor Shield anche dei pin femmina aggiuntivi nella zona della corrente elettrica e dei 6 piedini analogici. Noterete che la scheda ha la predisposizione per saldare dei pin extra. È importante ricordare che i pin analogici dell'Arduino possono funzionare sia in maniera analogica sia digitale. Sono segnati come digitalPin dal 14 al 19.

Non metteremo il jumper sui pin selettori di corrente (che si trovano a fianco della morsettiera a 2 poli per l'alimentazione) sul Motor Shield perchè intendiamo pilotare i motori e Arduino tramite due alimentazioni distinte, una soluzione comoda per garantirci maggiore flessibilità. Il setup corretto prevede il pin su Arduino (diecimila) impostato su EXT, e il pin sul Motor Shield non impostato. Se utilizziamo Arduino 2009 non è presente invece il pin per scegliere la sorgente di alimentazione e la scheda la imposterà automaticamente. A questo punto possiamo unire Arduino e il Motor Shield.
Per il nostro progetto utilizzeremo motori dc da 5V. Non è possibile indicare molte operazioni ai motori dc ma esclusivamente segnali base: avanti, indietro e la velocità. I motori dc sono di solito molto economici e si possono acquistare nei negozi di elettronica o di modellismo. Se tuttavia intendete seguire la vera strada hacker il mio consiglio è quello di smontarli da qualche vecchia apparecchiatura. Io ho utilizzato per il progetto motori ottenuti da vecchi lettori/masterizzatori cd o dvd. In ogni lettore sono presenti almeno un motore dc, qualche volta un motore stepper, un po' di resistenze e condensatori che probabilmente torneranno utili in altre occasioni.
Dopo aver sacrificato tre lettori cd alla scienza possiamo procedere ad attaccarli al Motor Shield. I cavi che escono dai motori vanno avvitati nelle posizioni M1, M2 e M3 del Motor Shield. Considerate che invertendo la polarità negativa con quella positiva il motore, ovviamente, cambia direzione. Sistemerete questi particolari nella successiva fase di test.

Attenzione, ogni motore dispone di una rondella di plastica incastrata sull'albero motore. Staccate le ron-



Per monitorare le vicinanze, il sensore sonar deve essee montato frontalmente.



Il dettaglio del sensore sonar SRF02 usato nel progetto: piuttosto economico e dalle dimensioni davvero contenute. I suoi possibili usi sono pressoché infiniti.

(Codice 1)

```
#define DELTA_TIME 1000  // Tempo che intercorre tra le letture del sonar
#define MOTOR1_GAP 300  // (cm) Il motore parte quando il sonar legge un valore più basso di questo
#define MOTOR2_GAP 200
#define MOTOR3_GAP 100

#define MAX_SPEED_MOTOR 150 // Velocità massima dei motori, valore compreso tra 0 e 254
#define MIN_SPEED_MOTOR 30 // Velocità minima dei motori, valore compreso tra 0 e 254
```

delle e tenetele da parte. Stampate le spirali e incollatele su cartoncino rigido, quindi ritagliatele. Stendete la colla sul cartoncino e non sulla spirale stampata per un miglior risultato. Per ogni spirale individuate il centro e posizionatevi (sulla parte posteriore!) la rondella precedentemente staccata dal motore. Per ottenere una maggiore robustezza, si consiglia di fissarla alla spirale tramite colla a caldo. Se desiderate fare prove più realistiche potete già attaccare le spirali agli alberi dei motori!

La parte mobile e visiva del progetto è stata completata. Scaldiamo il saldatore e passiamo all'installazione del sensore sonar, il punto cruciale del sistema. Per prima cosa saldiamo i pin maschi sul sonar SRF02. È una operazione semplice ma va svolta con una certa velocità, onde evitare di rovinare il sonar scaldandolo troppo col saldatore. A questo punto intestiamo dei cavetti con pin maschio e femmina ed utilizziamoli per collegare il sonar al motor shield.

Consultando il datasheet del sonar individuiamo i pin che indicano il +5 e il GND, e colleghiamoli correttamente su Arduino. I pin indicati con SDA e SCL vanno invece collegati rispettivamente ai pin analogici 4 e 5. I pin analogici 4 e 5 determinano su arduno diecimila e duemilanove il bus i2c, che è il bus utilizzato dal sonar per comunicare con la scheda.

Il bus i2c offre molte potenzialità! Tramite una singola coppia di fili potremmo collegare in cascata fino a 127 elementi hardware che lavorano in i2c. Nel nostro caso, trattandosi di un primo progetto, connetteremo esclusivamente il sonar. Tra il piedino +5 e il piedini SDA e SCL vanno saldate le resistenze di pullup per il bus i2c. Tali resisenze possono avere valori compresi tra 1.8KOhm e 4.7KOhm. Nella mia installazione ho utilizzato resistenze da 3.3KOhm ma non è escluso che possa funzionare meglio con altri valori: la bellezza dell'uso di un hardware open è che si possono sperimentare soluzioni alternative a quelle standard. Ora che la parte hardware è stata montata correttamente possiamo finalmente passare al caricamento del software su Arduino. Trovate il codice sorgente completo e pronto per essere compilato presso http://blackman.amicofigo.org/spiralipsichedeliche/indirizzofarlocco.

(Codice 2)

```
SRF02 sensor(0x70, SRF02_CENTIMETERS); // Indirizzo del sonar sul bus i2c
```

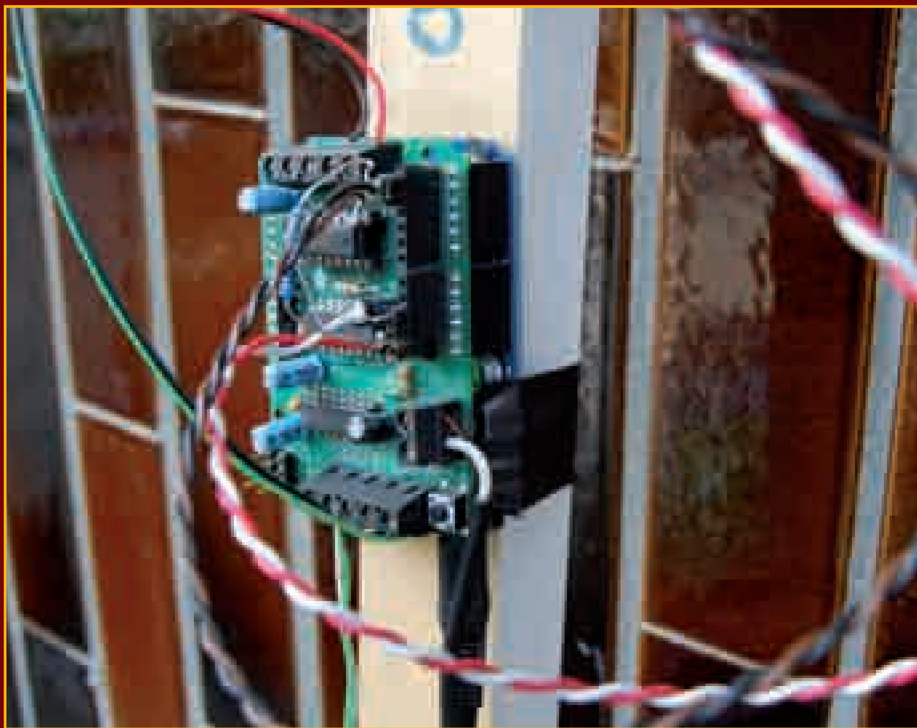
Per poter compilare correttamente il codice occorre prima installare le librerie di gestione dei componenti hardware motori e sonar. I file vanno copiati nella cartella di installazione di Arduino, in hardware/libraries. La liberia per il Motor Shield è scaricabile da www.Ladyada.net/make/mshield/download.html, mentre quella per il sonar SRF02 da www.grapelabs.de/index.php?id=51. Sui relativi siti vi sono anche alcuni esempi utili per testare i componenti singolarmente. Dando uno sguardo più attento al co-



Particolare della parte posteriore del montaggio, in cui si vede bene il motore della spirale e il retro del sensore sonar.



Il disegno frontale della spirale è già psichedelico quando il disco è fermo: immaginiamolo in movimento...



Sull'asta di sostegno trova posto il pacchetto hardware principale controllato da Arduino.

dice che gestisce le spirali notiamo che vi sono alcuni parametri di configurazione che possono essere modificati e testati (**Codice 1**).

La questione cruciale è il GAP che scegliamo. Le spirali non ruoteranno tutte contemporaneamente ma inizieranno a funzionare quando un oggetto si troverà più vicino di tre metri, in base alle impostazioni che abbiamo scelto. Ad esempio a distanza di 50 centimetri le girandole su MOTOR1 e MOTOR2 staranno girando a velocità massima e quella installata su MOTOR3 funzionerà a una velocità dimezzata (**Codice 2**).

Proprio in questa sezione di codice, invece, definiamo l'indirizzo 0x70 per il sonar sul bus i2c. Ricordiamoci che, qualora vi fossero più sonar, ognuno andrebbe pre-configurato con un valore diverso. Specifichiamo anche che i valori che il sonar ritornerà saranno in centimetri. È possibile utilizzare i parametri (autoesplicativi) SRF02_INCHES, SRF02_CENTIMETERS, SRF02_MICROSECONDS.

A ogni lettura del sonar il software imposta la velocità dei motori, che proseguiranno nel loro stato di moto fin tanto che una nuova lettura non ne varierà la configurazione. Una funzione chiamata a intevalli regolari si occupa del movimento vero e proprio dei motori (**Codice 3**).

[Codice 3]

```
void move_motor(AF_DCMotor *motor,int
start_at,int stop_at,int distance) {
  int quickness=0,motor_
state=FORWARD;

  if (distance<stop_at) {
    quickness=MAX_SPEED_MOTOR;
  }
  else if (distance<start_at) {
    quickness=(int)((start_at-
distance)*(MAX_SPEED_MOTOR/100.0));
  }
  else {
    motor_state=RELEASE;
  }
```

Alla funzione move_motor vengono passati un'istanza di un motore, i parametri di gap e la distanza letta dal sensore sonar. Chiamando ripetutamente questa funzione, Arduino regola la velocità dei motori che muovono le spirali. Grazie a questo metodo di controllo, potete inventare nuovi effetti di movimento in sostituzione di quello proposto. A questo punto non rimane che fissare i motori e arduno con Motor Shield ad un'asta di supporto e collegare l'alimentazione per vedere le spirali ruotare. È veramente importante utilizzare due alimentatori dc distinti per Arduino e per i motori onde evitare di danneggiare Arduino. Abbiamo finito: è il momento di portare la vostra installazione a una festa o di chiamare qualche amico per mostrare la vostra creazione!

Fede.Sideralis



Il montaggio ultimato e posto in funzione nella sua sede definitiva.



Ti conosco, caro OS

Scopriamo il sistema operativo di un computer grazie al "passive fingerprinting"

Come ormai dovremmo sapere a menadito, ogni sistema operativo ha le proprie tecnologie difensive. Firewall, antivirus, filtri anti-phishing e via dicendo, variano sensibilmente su Windows, Mac e sulle diverse distribuzioni di Linux. Per questo motivo, quando si tratta di operare un qualche "approccio" (chi ha detto "attacco"?) nei confronti di un computer, è prima essenziale conoscere il sistema operativo che utilizza. Ciò, è particolarmente vero perché le tecniche hacker basate su exploit si rifanno proprio alle vulnerabilità intrinseche in ogni sistema. E no, non esistono sistemi operativi privi di una qualche vulnerabilità. Per riconoscere il sistema operativo (o "OS") utilizzato da un computer-target, vale a dire il nostro obiettivo, ci sono svariate procedure e tecniche pronte all'uso, anche se la più efficace e utilizzata è il "passive fingerprinting". Si tratta di un metodo che riconosce l'OS di un host remoto analizzando alcune caratteristiche dei pacchetti TCP SYN, comparandole con un file, il "fingerprint file", appunto. Niente più che un elenco di parametri tipici di vari sistemi operativi. Così, in base alle coincidenze tra i dati dei pacchetti e quelli del file, si determina il tipo di sistema operativo.

:: Come CSI, anzi, di più

Lo stesso procedimento, insomma, dell'analisi delle impronte digitali che possiamo vedere in telefilm come CSI:

data un'impronta, la si confronta con un apposito archivio, sulla base di alcuni parametri, e si rilevano eventuali coincidenze. Ecco da cosa deriva il termine "fingerprint" utilizzato nella nostra situazione! Come detto, ci sono molti software utili allo scopo, anche se il migliore universalmente riconosciuto è P0f. E questo è vero, in particolare, per la sua più recente versione, la "v2". Questa, di fatto, consente di effettuare il passive fingerprinting verso:

- computer che si connettono al nostro terminale;
- computer ai quali siamo connessi noi;
- computer ai quali NON siamo direttamente connessi;
- computer che possono, genericamente, essere "osservati".

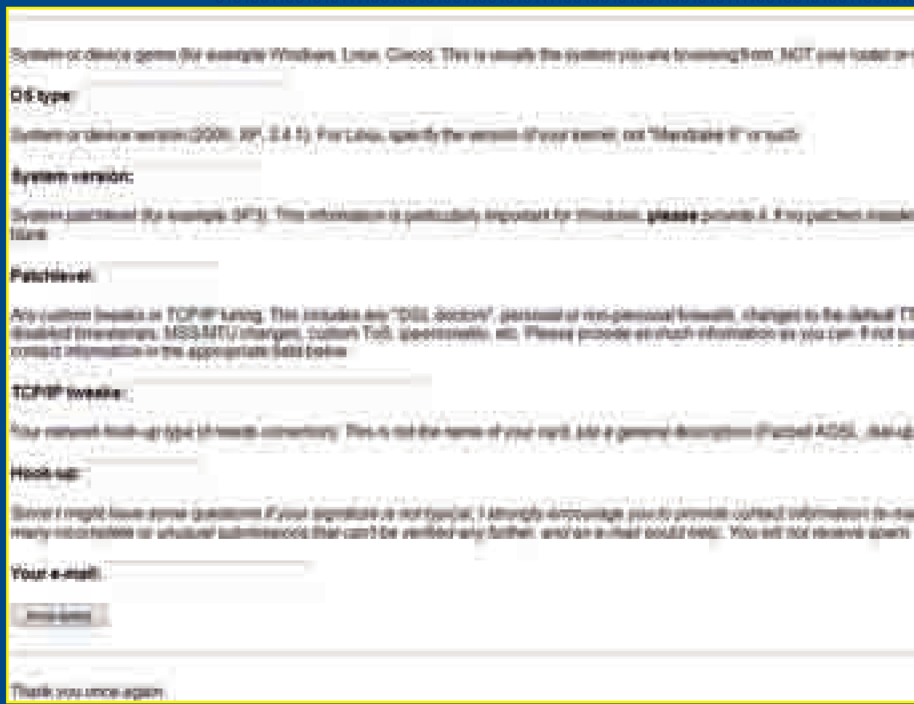
Ad aumentare la caratura del software in questione, ci sono molte altre chicche utili per hacker e appassionati. Tra le principali:

- capacità di determinare la presenza di un firewall, e della modalità NAT;
- determinazione della distanza tra il computer-target e il nostro, e il valore di uptime;
- determinazione del tipo di network utilizzato e dell'ISP.

Ovviamente, i risultati ottenibili variano molto in base a configurazioni, connessioni e situazioni varie e assortite, ma resta il fatto che ogni buon hacker, prima di applicare una qualsiasi tecnica di osservazione o intrusione, dovrebbe per lo meno effettuare una sessione di passive fingerprinting. Non di meno, questa tecnica è utilissima anche per chi si occupa di sicurezza delle reti, per verificare cosa un hacker può e non può rilevare con un software come P0f.

:: Come funziona P0f

Prima di passare a vedere l'utilizzo di P0f, vediamo nel dettaglio come funziona. Del resto, non siamo certo hacker da "pappa pronta", ma ci piace comprendere le tecnologie che stanno alla base degli strumenti che utilizziamo! P0f basa la sua potenza sui "fingerprint" forniti dai suoi stessi utilizzatori. Sono loro, infatti, a inviare le caratteristiche dei loro sistemi, in modo da arricchire l'archivio consultato dal programma stesso. Quindi, prima ancora di usare P0f per i nostri scopi, diamo un contributo al suo sviluppo. Per farlo, andiamo all'indirizzo http://lcamtuf.coredump.cx/p0f-help/. Una volta qui, compare un breve rapporto sulle caratteristiche rilevate nel nostro sistema. Qualche volta i dati rilevati via web sono errati, o imprecisi, quindi si deve compilare il semplice modulo sottostante, specificando tipo di sistema operativo (OS Type), versione (System version) e via dicendo. Terminato l'inserimento delle informazioni, inviamo il tutto, in modo sicuro, cliccando sul pulsante Invia query, a fondo pagina.



Compilando nel dettaglio questo modulo con i dati che ci riguardano, contribuiremo a migliorare ulteriormente l'efficacia di P0f. Più che una cortesia, è un nostro dovere…

:: Un utilizzo pratico

P0f si scarica, gratuitamente, dal sito ufficiale. Per i più pigri di noi, il link diretto è http://lcamtuf.coredump.cx/p0f.tgz. Una volta scaricato il file, scompattiamolo. Se utilizziamo Windows e non abbiamo un programma di decompressione, possiamo utilizzare Zipgenius, che troviamo su www.zipgenius.it. Secondo un'abitudine che non dovrebbe sconvolgerci più di tanto, l'archivio non contiene dei file binari, ma dei sorgenti scritti in linguaggio C. Si tratta di un C ben standardizzato, comunque, e la sua compilazione non crea particolari problemi: potremo usare la quasi totalità dei compilatori in circolazione ed ottenere un risultato immediato.

Comunque, se non vogliamo dare una sbirciatina al codice, se non abbiamo bisogno di modificarlo oppure abbiamo deciso di fare i pigri, troviamo dei binari piuttosto recenti su http://lcamtuf.coredump.cx/p0f/p0f-2.0.4-win32-binary.zip. Una volta compilato il programma, installiamo WinPCAP (www.winpcap.org), e quindi avviamo P0f. Il software si usa a riga di comando, secondo i parametri elencati e spiegati su http://lcamtuf.coredump.cx/p0f/README. Per la riuscita del passive fingerpriting, è essenziale specificare il file di fingerprint, che ha l'estensione FP, che accompagna sia i file sorgenti che i file binari di F0p.

Riccardo Meggiato

DIGITAL CAOS



Ci servirà più spazio accanto al televisore per tutti i decoder che dobbiamo comprare

Il giorno del 31 luglio 2009 è stata la fatidica data: ha ufficialmente preso il via l'offerta di tivùsat, la televisione digitale satellitare, nata con l'intento di contrastare lo strapotere monopolistico di Murdoch e del suo impero Sky. Il sito, www.tivu.tv, ci mostra tutti i dettagli e ci ricorda l'inesorabile calendario dello switch-over, ossia del passaggio dalla televisione analogica che abbiamo visto finora alla nuovissima televisione digitale. Il dubbio sta proprio nel termine "nuovissima": gira e rigira, se andiamo ad analizzare la situazione italiana con quella presente in altre parti del mondo, l'impressione che ci troviamo nel mezzo dell'età della pietra è sempre più forte.

:: L'era preistorica

La trasmissione televisiva, in Italia, è presente sin dal 1934, anche se è solo dal 1954 che ha inizio un servizio costante fornito dall'ente di Stato preposto (la RAI): fino ad allora si trattava di trasmissioni sporadiche e più che altro sperimentali. La diffusione su tutto il territorio nazionale però viene completata nel 1956 e gli abbonati erano solo pochi fortunati, visti i costi per l'acquisto dell'apparecchio ricevente. Se si fa eccezione per l'introduzione del colore, avvenuto nel 1977, la tecnologia è rimasta sostanzialmente la stessa nel corso di tutti questi 75 anni di vita. È chiaro quindi che non si tratta più di un servizio adeguato per le esigenze attuali degli spettatori, non tanto per quanto riguarda i contenuti ma semplicemente per motivi di scelta disponibile. Anzi, si può affermare con certezza che in Italia la scelta delle trasmissioni televisive è paurosamente in ritardo rispetto a quanto succede in



Uno dei primi modelli di televisore. Il gusto estetico dell'epoca voleva che si mimetizzassero con l'arredamento di casa.

altri Paesi: RAI 2 inizia a trasmettere solamente nel 1961, mentre RAI 3 tra il 1979 e il 1980, per non parlare dell'offerta privata che per oltre 20 anni è stata osteggiata dagli organi statali. Si parla in generale di una decina d'anni di ritardo rispetto ad altri Paesi europei più sviluppati per tutte le tappe fondamentali che hanno portato la trasmissione televisiva a essere quella che è oggi. Dal punto di vista tecnologico la solfa non cambia: sin dagli albori si è sempre trattato di trasmissioni analogiche su frequenze radio, con tutti i problemi di interferenze, coni d'ombra e riflessioni tipici, che ci siamo portati dietro fino a oggi.

:: L'alternativa

Parliamoci chiaro: le tecnologie in Italia non decollano perché esiste di fatto una sorta di monopolio nell'ambito delle trasmissioni, che è tale perché esiste ancora un organo statale (sia per quanto riguarda la sua costituzione, sia per quanto riguarda il suo controllo) che è privilegiato rispetto ad altre offerte. Chiunque in Italia volesse far partire una nuova offerta di intrattenimento e divulgazione via etere, si troverebbe in difficoltà sin dalle prime battute proprio a causa delle restrizioni e dell'osteggiamento di chi conserva la posizione predominante (e non stiamo parlando nel particolare di RAI, Mediaset o quant'altro, ma dell'establishment effettivo che nell'insieme costituisce l'offerta attuale in Italia, intenzionato a conservare per sé il mercato nella sua globalità). Pensiamo alle difficoltà iniziali nella diffusione di una tecnologia come quella della televisione satellitare, oggi alla portata di molti (non ancora per tutti, visti i costi di installazione degli apparecchi necessari e di abbonamento al servizio). Anche in questo caso, però, siamo giunti a una situazione di monopolio nemmeno tanto teorico, dato che la totalità dell'offerta satellitare nel nostro Paese è nelle mani di Sky. Comunque un'alternativa, anche se relegata a status symbol elitario.

:: Lo switch-over

Nel pieno dell'era dell'informazione, continuare imperterriti a usare una tecnologia analogica sa quasi di blasfemia: ecco quindi apparire il Digitale Terrestre e il fatidico momento dello switch-over, ovvero del passaggio dall'analogico al digitale. Mirabolante novità o stessa minestra riscaldata? Analizziamolo un momento: la trasmissione avviene sempre mediante onde radio, così come avveniva per la televisione analogica che abbiamo usato finora, ma



Un ripetitore televisivo analogico: se siamo oscurati da un ostacolo anche non naturale, la nostra ricezione risulta difficoltosa.



Dobbiamo comprarne uno: è un decoder per la televisione digitale terrestre. Ma forse non risolverà i nostri problemi di ricezione.

i dati trasmessi non sono più variazioni di segnale senza soluzione di continuità modulate da una portante in radiofrequenza. Ciò che viene trasmesso è un pacchetto di dati digitali che, opportunamente decodificato, viene riconvertito in segnale audio e video per la riproduzione nel comune televisore di casa. L'aspetto fondamentale del cambiamento non è tanto nella tecnologia usata, che tutto sommato non è dissimile alla trasmissione in streaming che già avviene su Internet da diverso tempo, ma nel fatto che per la sua fruizione occorre un dispositivo da affiancare al televisore. La scocciatura, se così la si può chiamare, è che non si tratta di una scelta facoltativa: è una decisione ministeriale che obbliga tutti gli utenti ad aggiornare la propria strumentazione, comprando un decoder a parte oppure cambiando il televisore per comprarne uno che lo integri.

Tutto sommato non è un male, la qualità della ricezione è notevolmente migliorata così come la scelta tra i canali e le trasmissioni disponibili, ma ci domandiamo perché anche in questo caso siamo rimasti a fare da fanalino di coda dello sviluppo tecnologico dei paesi più avanzati. Perché solo ora si parla di televisione digitale, quando da almeno un decennio in altri Paesi tecnologie come la televisione digitale via cavo sono una realtà alla portata di tutti? Comunque, lo switch-over continua secondo la tabellina di marcia indicata dal Ministero, che pubblichiamo in queste pagine. Non tutti quindi possono ancora fruire della nuova tecnologia, e non tutti lo potranno fare nemmeno quando il passaggio al digitale sarà definitivo su tutto il territorio nazionale, a causa dei problemi

di trasmissione terrestre (l'Italia è pur sempre un Paese che convive con alte catene montuose difficili da superare anche per le onde radio).

:: Tivùsat

Ecco quindi che, con lo switch-over non ancora terminato, vediamo spuntare dal nulla una nuova offerta televisiva: la televisione digitale satellitare, per raggiungere anche quei posti in cui non è ancora stato attivato il digitale terrestre e che saranno difficilmente raggiungibili anche quando questa tecnologia arriverà alla sua piena operatività. Che diamine. Se il digitale satellitare raggiunge tutti indistintamente, perché dobbiamo passare dal digitale terrestre? Chiaro, sono due tecnologie differenti e si può sempre scegliere di non usufruire del terrestre se si dispone già di una parabola per la ricezione di Sky. Ma servirà comunque un altro decoder, costo circa 100 euro. Un'altra scatoletta accanto al televisore, un altro telecomando, confusione su chi può vedere cosa, dubbi sul fatto che certi canali siano gratuiti o no e un gran mal di testa finale. Soprattutto perché alla fine saremo costretti a comprare tutto, se vogliamo essere certi di poter guardare la TV in santa pace. La RAI vuole uscire da Sky per seguire solo il digitale satellitare, Murdoch non ci sta e le associazioni dei consumatori si ribellano contro i canoni troppo alti (una nota per chi ha scritto l'articolo su Wikipedia: la RAI non si sovvenziona solo con contributo statale e pubblicità, ma anche con i soldoni che ogni anno spilla a tutti gli italiani, una piccola dimenticanza...): ecco la realtà televisiva oggi in Italia.



Il sito www.tivu.tv è l'organo ufficiale del nuovo consorzio che gestirà il digitale satellitare.

CALENDARIO NAZIONALE

2008	II sem	Area 16 Sardegna
2009	I sem	Area 2 Valle d'Aosta
	II sem	Area 1 Piemonte occidentale Area 4 Trentino e Alto Adige *(inclusa la provincia di Belluno)* Area 12 Lazio Area 13 Campania
2010	I sem	Area 3 Piemonte Orientale e Lombardia *(inclusa la provincia di Piacenza)*
	II sem	Area 5 Emilia Romagna*

La tabella di marcia per il passaggio al digitale terrestre, diviso zona per zona.

:: Il quinto potere

Non è facile districarsi tra tutte queste offerte, non lo è per chi un po' mastica la tecnologia, figuriamoci per la signora Pina di Voghera che vuole solo vedere Mike Bongiorno ma non sa più dove andare a pescarlo. Purtroppo, così come avviene per la carta stampata, la libertà nel mondo televisivo è soltanto un'utopia: il potere che è nelle mani di chi è in grado di controllare le informazioni è troppo forte e, in un mondo in cui tutto è guidato da scelte commerciali (in sostanza, tutto si fa solo se porta soldi), poco importa se a farne le spese sono gli utenti comuni. Al potere dell'informazione sono collegati direttamente, e non solo nel nostro Paese, il potere politico e quello commerciale. Non saremo mai noi a scegliere veramente che cosa vedere e come intrattenerci nelle lunghe serate invernali: l'unica maniera sarebbe rinunciare completamente alla televisione e optare per passatempi più intelligenti, fino a quando non troveranno il modo di controllare anche quelli. E di farci comprare un decoder anche per giocare a briscola.

Largo al download

Che ne direste di un router Wi-Fi che scarica file al posto vostro e può essere personalizzato?



Fon è per prima cosa una community, diffusa in tutto il mondo, composta da utenti che condividono tra loro la connessione a Internet. È la community di questo genere più diffusa grazie alla politica commerciale adottata: non solo prevede livelli di partecipazione diversi al progetto in base alle esigenze di ogni utente ma vende anche il necessario per entrare a far parte della comunità. In origine, Fon si fece notare perché tramite il suo sito vendeva a prezzo di costo dei router Linksys già configurati per la condivisione della connessione. In seguito al successo riscosso dall'iniziativa, venne creata una versione speciale di router, sempre venduto tramite il sito, adattata alle esigenze della community. Dopo un aggiornamento del software e un restyling, Fonera è stata ripresentata con la sua versione 2.0: un router Wi-Fi, con caratteristiche simili alla versione precedente quali la divisione tra rete pubblica e dominio privato col supporto di due SSID, sistemi di sicurezza vari, gestione della sezione pubblica direttamente da parte dei tecnici della community e così via. A metà luglio, Fon ha presentato un ulteriore aggiornamento, che verrà probabilmente venduto a partire da ottobre e il cui costo sarà inferiore ai 100 euro. Il nuovo router Fonera 2.0n dispone di un hub USB integrato che permette di mettere in comunicazione la rete Wi-Fi con diversi accessori: hard disk ma anche stampanti, webcam o persino dongle HSDPA e 3G. Nello specifico, la possibilità di collegare un disco USB a un router permette di trasformarlo, de facto, in un disco di rete, raggiungibile da qualsiasi altro computer della LAN, sia wired che wireless. Grazie a un core piuttosto evoluto, Fonera 2.0n permetterà il collegamento, a computer spento e con un disco USB collegato, con sistemi di upload e download come Bit Torrent ma non solo: è stata posta particolare attenzione al mondo dei social network permettendo una interfaccia naturale con YouTube, Flickr, Picasa e Facebook. D'altra parte, la possibilità di collegare una chiavetta HSDPA aprirà scenari interessanti anche per chi non ha una connessione ADSL classica. La novità più golosa di Fonera 2.0n, però, sta in quella "n" che la distingue dalla versione precedente: supporta lo standard 802.11n. Annunciato nel 2004 e tutt'ora in fase di standardizzazione, l'802.11n promette velocità di 100 Mb/s e risulta 5 volte più rapido dell'attuale 802.11g e ben 40 volte più veloce del più diffuso 802.11b. Una novità che fa gola considerando che l'accessorio non dovrebbe costare più di 100 euro e che l'inserimento del supporto a sistemi di trasmissione così veloci non sarà disponibile, almeno inizialmente, sui prodotti di fascia equivalente. Un motivo in più, forse, per entrare nella community Fon.

NUVOLE DI VELENO?



L'ultima frontiera della lotta tra i big dell'IT è la fornitura di servizi di cloud computing. Ma interessa a qualcuno?

Metteresti i tuoi dati personali in una cassaforte lontana migliaia di Km, in un luogo che nemmeno tu conosci e gestita da anonimi impiegati? Ci metteresti anche il bilancio della tua società, la tua posta elettronica, il tuo diario dei ricordi, l'elenco dei fornitori, quello dei clienti e chi più ne ha, più ne metta? Detta così, la questione non è propriamente di facile soluzione e sicuramente più di un commerciale ha storto il naso per come viene posta. Però, la questione è tutta qui: il cloud computing, ultima frontiera della lotta tra i big dell'IT, non è altro che questo.

La linea è stata tracciata da Google, che fornisce in remoto una serie di servizi gratuiti o a prezzi estremamente concorrenziali ma tutti gli altri big sono partiti quasi contemporaneamente oppure sono nella sua scia.

Il concetto è banale e vecchio quanto l'IT moderna: invece di avere in casa un hardware costoso, acquistare licenze per il software, dotarsi di attrezzature complementari e pagare una costosa manutenzione è possibile affidarsi a una società specializzata che gestisce tutto al posto nostro. Naturalmente, questa società è attrezzata per farlo: computer potentissimi, configurazioni in cluster, farm dotate degli ultimi ritrovati in campo di sicurezza e protezione dei dati, di connessioni velocissime, di soluzioni software all'avanguardia e via dicendo.

:: Imprenditori?

Ovviamente, la concentrazione di applicazioni permette di ridurre notevolmente i costi e quindi di affittare spazio e potenza di elaborazione a una frazione infinitesima rispetto a quello che si verrebbe a spendere occupandosi direttamente della cosa. Persino l'affidabilità è più



La sede di Google è uno dei luoghi fisici dove sono ospitati i dati della sua cloud. Non è proprio a due passi: dista 9000 Km dall'Italia.

alta: se in teoria le aziende devono garantirsi un certo livello di protezione e di continuità, la stragrande maggioranza delle aziende, specialmente italiane, va molto al risparmio su questi temi. Ovvio, quindi, che la proposta di mettere i propri dati nella "nuvola" faccia gola a molti imprenditori. C'è offerta, c'è domanda... Ma il servizio non sembra nascere sotto gli auspici migliori. Il motivo è quello che si intuisce dalla domanda con cui abbiamo iniziato: dove finiscono i nostri dati? È questo, in fondo, che frena la domanda del mercato, che fa nascere ben più di una perplessità e che impedisce a un imprenditore di affidarsi a questo servizio a cuor leggero.

Al di là della rispettabilità dell'azienda che propone il cloud computing, il pensiero che uno sconosciuto possa leggere informazioni vitali per l'azienda e farci sostanzialmente quello che vuole è un blocco non indifferente. Per chi non è del settore informatico è difficile convincersi che un fornitore non possa essere allettato dalla lettura di documenti tecnici, procedure aziendali, elenchi di fornitori, processi industriali e quant'altro forma un'azienda: c'è il rischio che le idee, vera ricchezza aziendale, possano sfuggire e passare nelle mani dei concorrenti. Concorrenti che, a loro volta, potrebbero aver affidato i loro dati allo stesso fornitore, aprendo scenari di spionaggio industriale degni di un romanzo. Attenzione, con questo non si accusa Google, Microsoft o i loro concorrenti di svolgere operazioni occulte ma si intende segnalare un rischio che non può essere escluso in modo assoluto: persino senza coinvolgimenti da parte di eventuali "basisti", l'hacking di password su sistemi pubblicamente raggiungibili è un terreno piuttosto ricco di precedenti. Dal furto di account al phishing, gli esempi si sprecano.

La maggior parte degli imprenditori italiani ha un'azienda perfettamente in target con l'offerta ma ha anche un bisogno di fisicità che va ben oltre la logica: in diverse aziende vengono messe protezioni fisiche insormontabili per l'accesso in sala server per poi lasciare prese di rete abbandonate in corridoio, reti WLAN aperte, password di amministrazione che non cambiano per anni, firewall senza aggiornamenti e via dicendo. Ci sono persino imprenditori che si fanno mettere i server in stanze attigue al loro ufficio, per tenerli sotto controllo, quasi che per il furto di dati o la loro distruzione sia necessario metterci sopra le mani. L'importante per loro è che il server, identificato nella sua fisicità, sia al sicuro. È per questo motivo che i dubbi sulla diffusione del cloud computing come viene inteso attualmente sono legittimi e non sarà facile far digerire questi dubbi agli



Chi dice Amazon, dice libri e mille altre cose... Tra cui una delle più diffuse piattaforme di cloud computing.



Azure è la proposta di Microsoft di una piattaforma di sviluppo di applicazioni nella nuvola: per ora non è ancora molto diffusa.

imprenditori non solo italiani: la realtà mondiale della piccola imprenditoria non è molto diversa dalla nostra.

:: In Italia non si può

Da noi, semmai, ci sono altri problemi che si sommano alle considerazioni appena viste. Il principale è probabilmente la scarsa qualità delle connessioni a Internet: a fronte di zone coperte in fibra ottica da più operatori, gran parte del paese è servito da connessioni xDSL di bassa qualità mentre altre non sono servite affatto. La diffusione di una Internet veloce, inoltre, non dipende nemmeno dalla distribuzione industriale sul territorio: al di fuori delle cinture periferiche delle grandi città ci sono complessi industriali notevoli, in cui le uniche connessioni sono le ADSL oppure, addirittura, le connessioni tradizionali via modem. Complessi industriali in cui è già complicato riuscire a inviare e ricevere messaggi di posta elettronica: vi immaginate cosa succederebbe con un accesso massiccio e obbligatorio a servizi come Google Documents? Oppure con la necessità impellente di stampare un report di svariate centinaia di pagine, frutto dell'elaborazione di un programma che gira su un server fisicamente collocato dall'altra parte del mondo quando l'unica ADSL disponibile è condivisa tra decine di impiegati?

Linux sulla Vodafone Station



Liberiamo il pinguino che si cela nella Vodafone Station e creiamo un dispositivo dalle potenzialità infinite

La natura dell'hacker si sa, è quella di voler metter mano agli oggetti per capirli meglio e avere sicuramente maggior vantaggio dal loro uso, ma indubbiamente l'aspetto ludico è spesso la molla stessa dello "smanettone". A volte poi capitano per le mani dei gioielli tecnologici anche a buon prezzo, che riescono a stimolare maggiormente quella voglia di capire cosa c'è dietro, magari perché si scopre abbastanza presto che chi lo vende e distribuisce ha fatto di tutto per bloccarlo e limitarlo e questo non ci piace.

È il caso della Vodafone Station (VS), alias Huawei EchoLife HG553, router che viene regalato ai sottoscrittori dell'offerta ADSL del gestore telefonico e che è un concentrato di nuove tecnologie, disponendo di un hub integrato di 4 porte ethernet, 2 porte telefoniche che permettono di instradare le chiamate indifferentemente su rete cellulare e ADSL 2+, 2 porte usb in una delle quali va inserito un modem hsdpa fornito a corredo ed è al tempo stesso un access point wi-fi 802.11g. Ma l'informazione più importante è tenuta nascosta: al suo interno è presente una versione embedded di linux ed è possibile sbloccarne le potenzialità (**Figura 1**).

:: Limiti del firmware pre-installati

La VS dispone di un'interfaccia web che permette di selezionare un numero limitato di funzioni. Basti pensare che non è possibile cambiare il SSID della rete wifi, né la chiave di crittazione e come si legge nella documentazione, il gestore si riserva di aggiornare automaticamente da remoto il firmware del dispositivo senza alcun preavviso. Dall'interfaccia è possibile visualizzare le funzionalità samba, per la condivisione di stampanti o dei dati di un eventuale memoria esterna (es. pen drive o hard-disk su porta usb), ma quando si va nella sezione ftp si scopre che l'accesso è in sola lettura e per copiare i file deve per forza essere usato il trasferimento via windows (abbastanza immediato con XP, da mal di pancia con Vista, ma questa è un'altra storia), per partizioni fat/fat32. Per partizioni ntfs l'accesso è in sola lettura anche via samba!
Sapendo che all'interno della VS c'è Linux (ma certo Vodafone non ci informa), ci si aspetterebbe come minimo la possibilità di avere un console, che in effetti è disponibile, ma nascosta. Anzi, leggendo in rete si scopre che per esplicita richiesta di Vodafone a Huawei tutti gli accessi al sistema interno debbono essere bloccati per l'utente finale. L'hardware deve svolgere solo il compito che Vodafone vuole, quello di gestire la connettività. Ma come si legge nel contratto che si sottoscrive per avere la VS, l'utente è proprietario dell'apparato. Quindi perché limitarci a usarla "solo come router"? Non sarebbe per esempio più divertente farla diventare un server eMule o torrent da gestire anche da remoto? Per non parlare del fatto che non è possibile usarla con un altro gestore ADSL, non possono infatti essere cambiati i parametri di connessione.

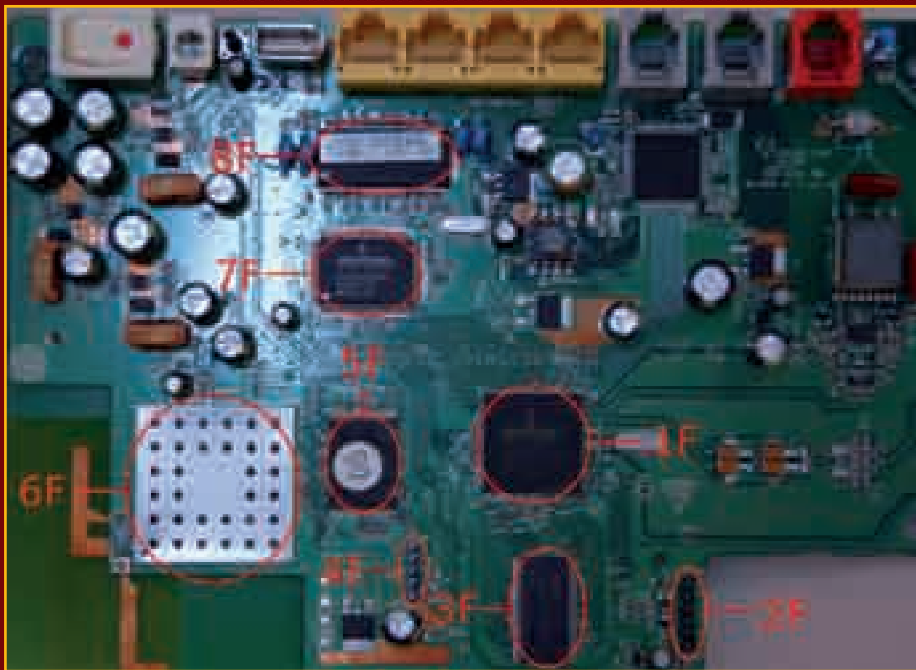


Figura 2: motherboard di HG553: CPU (1F), USB (2F), flash (5F), ethernet switch (8F), ram (3F), circuit for VoIP (3F), antenna (6F), 5 pins headers, soldered (4F), 10 pins (1B), buffer (2B).



Figura 1: la VS oltre ad avere molte porte monta un processore dual-core MIPS da 300MHz, 64Mb di RAM e 16Mb flash.

:: Assalto alla Bastiglia

Liberare la VS per usarla anche con altri gestori ADSL è esattamente quello che ha pensato di fare Giovanni Gatta, che ha realizzato un sito web (http://tails92.sepwich.com/files/vstation) dove ha riportato l'hacking realizzato sul sistema per riuscire a capire dapprima come era costruito e poi come poterlo addomesticare (**Figura 2**). In particolare è stato scoperto in breve tempo che nella VS è installata una versione embedded di linux che dispone di due sole console e il cui accesso dall'esterno è stato bloccato con le versioni di firmware successive a quella di dicembre 2008.

Per verificare immediatamente la presenza o meno del blocco è sufficiente lanciare un telnet 192.168.1.1 da linea di comando di un PC connesso alla VS, via lan o WI-FI. Se l'accesso viene rifiutato abbiamo sicuramente un firmware recente a bordo e il primo passo per liberare la VS è quindi quella di effettuare un downgrade.

:: Downgrade del firmware

Supponendo di avere una versione recente, va scaricato il firmware "patchato" che mantiene il telnet funzionante (tails92.sepwich.com/files/vstation/freddy77_mirror/dl/image_b33.bin.bz2). Una volta decompresso l'archivio sul nostro PC, otteniamo il file "image_b33.bin" e possiamo procedere all'aggiornamento:

1. va spenta la VS;
2. tenendo premuto il tasto di reset la riaccendiamo e manteniamo il reset premuto almeno un minuto (durante questo tempo la VS effettuerà il boot, ma si predisporrà in una modalità che permette di aggiornare il firmware);

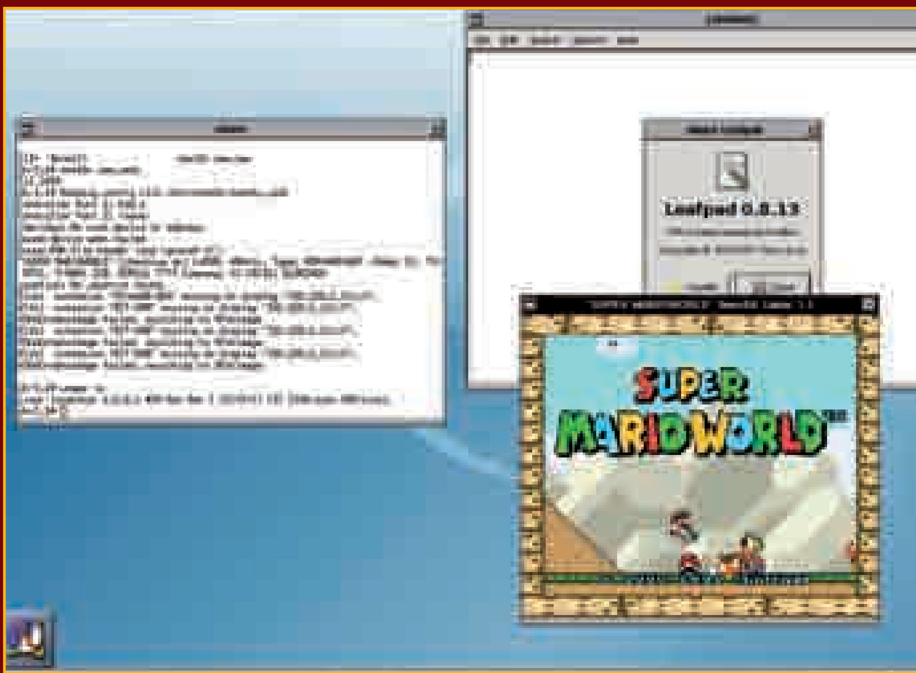


Figura 3: ecco come si presenta l'output di X in funzione sulla VS visto dal client.

3. dal client apriamo Firefox (con Internet Explorer non è garantita correttamente la funzionalità) all'indirizzo 192.168.1.1 e verrà visualizzata una semplice pagina in cui viene richiesto di caricare il firmware esterno (se ciò non accade ripetiamo da 1 e teniamo il reset premuto più a lungo);
4. indicheremo il percorso dove abbiamo decompresso la versione di dicembre e diamo upload.

Il processo è relativamente breve, ma se qualcosa dovesse andare storto non è garantito che la VS sia recuperabile e Vodafone stessa potrebbe non riconoscere la garanzia sull'apparato compromesso. In questo caso si potrebbe tentare di ripetere la procedura di downgrade per ripristinare la flash o come ultima spiaggia usare un programmatore esterno.

Supponendo che tutto sia andato a buon fine, la VS si riavvierà e potremo verificare il corretto funzionamento ricaricando la pagina sempre dal nostro client. Ora il telnet sarà abilitato e potremo accedere finalmente a Linux: login e password sono impostati di default a "admin", quindi il consiglio spassionato è quello di cambiare la password per ovvie ragioni e di ricordare bene la nuova che non c'è modo di recuperare a meno di un riaggiornamento del firmware. In particolare gli utenti cui cambiare la password sono: admin, support e user. La procedura è semplice: ">passwd <user> <password>".

:: Linux sulla VS

Ora che la VS è liberamente accessibile possiamo scoprire autonomamente che effettivamente è presente una versione di linux 2.6 compilata per processori MIPS, con il root in sola lettura e supporto nativo solo per filesystem fat/fat32/ntfs. Dopo il login via telnet ci troviamo in una busybox con pochi comandi, ma dando sh ci ritroveremo una shell di Linux.

Possiamo studiare un po' la struttura che è stata data al filesystem, la documentazione presente e identificare diversi binari che gestiscono in modo chiuso le connessioni di rete e SIP. Ma soprattutto verificheremo che non possiamo fare molto e per aggiungere la possibilità di scrivere nel filesystem dobbiamo per forza passare per la usb libera (l'altra è occupata dal modem hsdpa).

:: La prova

Dopo alcune prove fatte con una pendrive, ho partizionato un hard-disk esterno da 500Gb in questo modo:

1. 499Gb come partizione dati, formattato in ntfs;
2. 1Gb per Debian, la mia distro preferita, in versione MIPS, formattato in ext2.

Nella partizione ntfs (/dev/sda1) ho creato una cartella "_VS_" in cui ho decompresso il modulo ext2.ko compilato per MIPS (da tails92.sepwich.com/files/vstation/vsstuff.tgz), mentre nella root ho realizzato uno script che esegue le operazioni iniziali da eseguire al boot della VS per abilitare la partizione ext2. Lo script si trova nella partizione ntfs che è supportata nativamente, mentre quella ext2, finché non viene caricato il modulo, non può essere nemmeno vista.

In particolare oltre a dover caricare il modulo, vanno creati anche i device associati alla partizione che si vuole montare (nel mio caso "mknod /dev/sda2 b 8 2").

Nella partizione ext2, ho decompresso il root compilato da Debian Etch (tails92.sepwich.com/files/vstation/vsroot.tgz) e dopo aver collegato l'hard-disk alla VS ho montato la partizione in /var/mnt/mylinux. Una volta caricata, va lanciato lo script ./chrooted e dopo qualche istante siamo in bash con un sistema linux montato in rw!



La VS è progettata per rimanere sempre accesa, ma può capitare che salti la corrente o si debba spegnerla per qualche motivo. In quel caso, la configurazione "chroo-

ted" salta e vanno ripetuti i passaggi precedenti, per questo suggerisco di utilizzare uno script. Nel caso invece che si venga semplicemente disconnessi da telnet, dopo un nuovo collegamento è sufficiente rilanciare lo script chrooted.

:: Linux in rete

La Debian ha il fantastico apt-get per gestire i pacchetti e va considerato che il root che ci troviamo non ha tutti gli strumenti che potremmo essere abiutati ad usare.



Da un client connesso alla VS lanciamo quindi la connessione a internet caricando l'home page 192.168.1.1 e cliccando su Connetti e una volta in rete nella console telnet diamo subito un bel "apt-get update". Per qualche strana ragione, se decidiamo di aggiungere un qualunque pacchetto nella shell di default incontriamo degli errori. Per questo va inserito ksh: prima di lanciare "apt-get install <nuovo pacchetto>" diamo ksh e al prompt possiamo procedere. Chiaramente una volta installato possiamo fare logout e ritrovarci in bash.



Uno dei problemi legati al collegamento telnet, purtroppo, è quello di venir disconnessi dopo un certo periodo di inattività e di dover rilanciare il chroot una volta riconnessi. Cambia notevolmente il discorso se invece riusciamo a eseguire una sessione X e a esportare lo schermo dalla Station al nostro computer.

Chiaramente il client deve avere un server X ove visualizzare le finestre in run sulla VS ed è quindi quasi obbligata la scelta di avere Linux su quel client, ma è possibile installare X anche su Windows, ad esempio tramite Cygwin.

Supponendo di avere un client con Ubuntu, sulla VS tramite apt-get dobbiamo dapprima installare X e almeno un window manager come twm (apt-get install xserver xbase-clients twm), dopodiché diamo il comando "export DISPLAY=192.168.1.2:0" dove al posto dell'indirizzo di rete dobbiamo mettere quello del nostro client e il ":0" indica la prima schermata disponibile (**Figura 3**).
A questo punto sulla VS con il comando "nohup twm&" verrà lanciato in background sulla VS il window manager che visualizzerà la finestra nel nostro client Ubuntu. Da questa finestra possiamo pilotare la VS e non occorre più la connessione telnet che possiamo terminare. Installiamo aMule (apt-get install amule) sulla Vodafone Station e lanciamolo: ora possiamo verificare le prestazioni della rete e mettere in download i file direttamente sul nostro hard-disk esterno! (**Figura 4**).

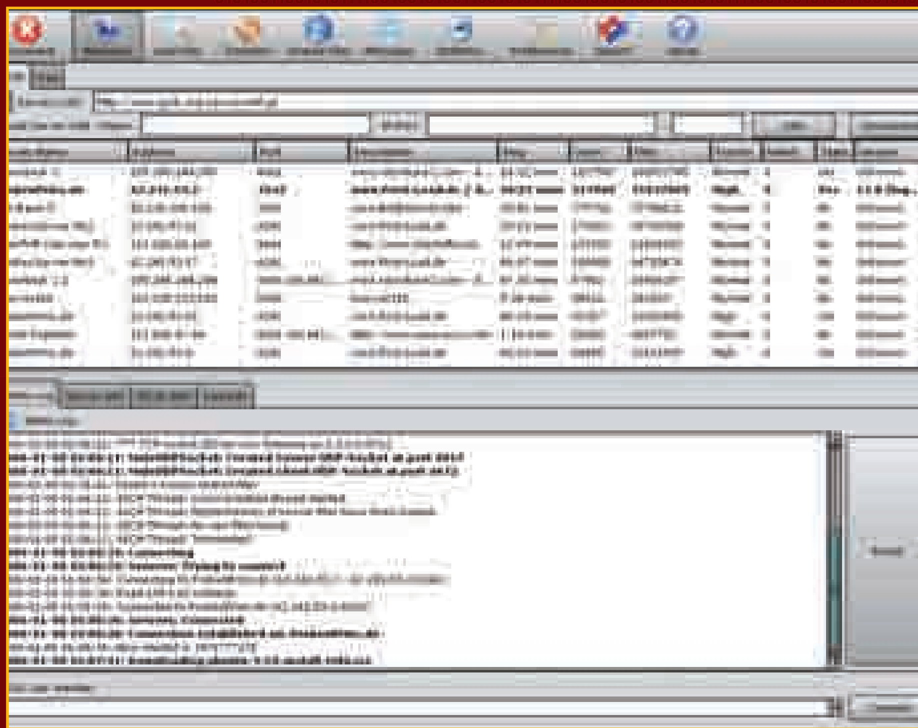


Figura 4: aMule è una delle incarnazioni del più famoso eMule, compilato per linux.

Massimiliano Brasile

aMule gestito da remoto



Controlliamo da una postazione remota aMule, il client eMule per GNU/Linux, utilizzando un semplice web browser

Il programma aMule, noto client eMule per sistemi GNU/Linux, presenta senz'altro un'interfaccia grafica completa e piena di opzioni, grazie alla quale ricercare e scaricare file dalle reti P2P EDonkey e KAD è davvero semplicissimo. Eppure, c'è una mancanza nell'interfaccia di aMule come, del resto, in quella di gran parte dei client eMule: non è possibile gestire gli scaricamenti da remoto. Sarebbe utile, infatti, poter controllare il funzionamento del programma da una postazione remota, magari tramite una semplice interfaccia web accessibile da qualsiasi dispositivo connesso ad Internet. Viene in nostro soccorso amuleweb, un vero e proprio web server che ci permette di accedere ad aMule dalla Rete mediante un browser: scopriamo, quindi, nei paragrafi che seguono come installare e configurare questo web server minimale. La distribuzione GNU/Linux presa come riferimento è Ubuntu 9.04 Jaunty Jackalope.

:: Installazione e primo avvio

Per poter usare amuleweb dobbiamo installare anche amuled, una versione di aMule senza interfaccia grafica che va avviata al boot del PC (si tratta dunque di un "demone"). Innanzitutto, quindi, scarichiamo dalla Rete ed installiamo i due programmi con un unico comando: apriamo una console di terminale e lanciamo "sudo apt-get install amule-daemon", dopo esserci sincerati che la connessione ad Internet sia attiva. Fatto questo, nel terminale lanciamo "amuled": il programma genererà la directory di configurazione di aMule, se questa è assente, e quindi si chiuderà segnalando un errore (**Figura 1**).

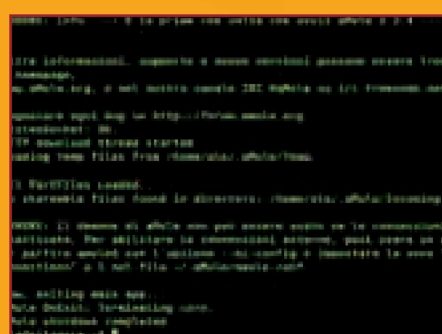


Figura 1: Eseguiamo una volta "amuled" per creare la directory di configurazione.

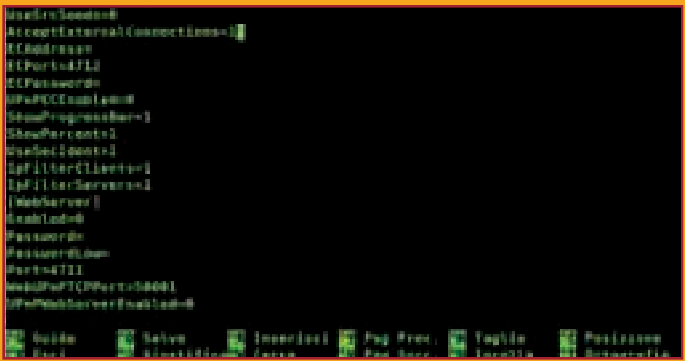


Figura 2: Entriamo nel file amule.conf per configurarlo a dovere.

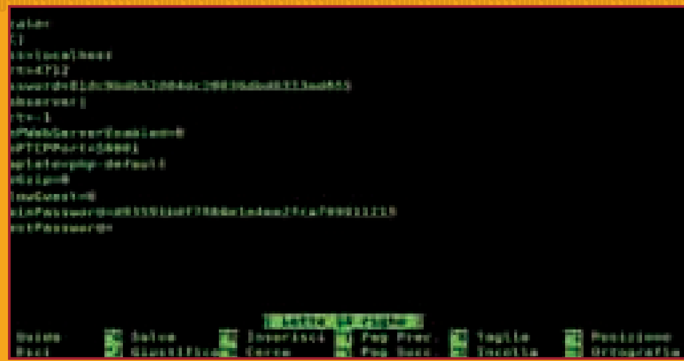


Figura 3: Modifichiamo remote.conf per configurare il web server.

:: La configurazione, primi passaggi

Assicuriamoci che nel firewall presente sul sistema sia possibile accedere dalla rete esterna alla porta 65535: se ci colleghiamo ad Internet tramite router ADSL, ad esempio, entriamo nell'interfaccia web per la configurazione del router e, in questa, apriamo la porta TCP 65535 per l'indirizzo IP del PC su cui lanciamo amuleweb. Ora possiamo alla configurazione di amule. Apriamo con un editor il file amule.conf: per fare ciò nel terminale eseguiamo il comando "nano $HOME/.aMule/amule.conf". Nel file cerchiamo la riga che inizia con "AcceptExternalConnections" e facciamola diventare come in Figura 2:
AcceptExternalConnections=1

:: Generiamo la password

Rimanendo sempre all'interno del file amule.conf, cerchiamo la riga "ECPassword=". Qui dobbiamo inserire la password per accedere ad amuled dal web server amuleweb; la password va inserita calcolandone l'hash md5 e copiando questo come argomento dell'opzione ECPassword. Per calcolare l'hash md5 entriamo in una nuova console di terminale e lanciamo il comando seguente, digitando al posto di 1234 la password da noi scelta:
echo -n 1234 | md5sum

Comparirà una riga di output: la prima sequenza di caratteri presente è l'hash che cerchiamo. Inserita questa sequenza nella riga "ECPassword=" (ad esempio, "ECPassword=81dc9bdb52d04dc20036dbd8313ed055"), salviamo il file amule.conf premendo Ctrl + O ed Invio e quindi usciamo dall'editor con Ctrl + X.

:: La configurazione del web server

Terminata la configurazione del demone amuled, occupiamoci di quella del web server. Nel terminale lanciamo il comando "amuleweb -w": questo genererà il file di configurazione di amuleweb, remote.conf. Apriamo questo file con l'editor, eseguendo il comando "nano $HOME/.aMule/remote.conf". Individuiamo la riga "Password=" ed aggiungiamo, in questa, l'hash md5 della password che abbiamo precedentemente inserito in amule.conf. Fatto questo, dobbiamo stabilire la password che sarà richiesta per ottenere l'accesso da remoto all'interfaccia del web server. Generiamo, anche in questo caso, l'hash md5 della password tramite il comando md5sum ed inseriamolo nella riga "AdminPassword=".

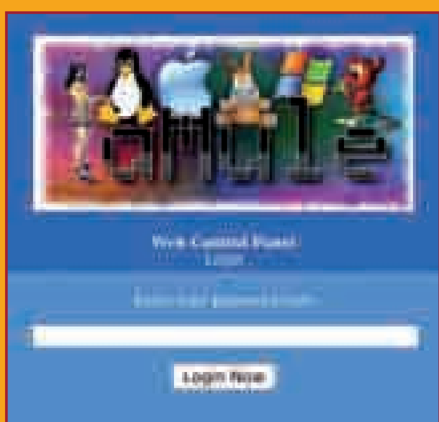


Figura 4: La pagina schermata iniziale dell'interfaccia Web di amuleweb.

Poi salviamo le modifiche al file e chiudiamo l'editor (Figura 3).

:: Avvio al boot

Ora facciamo in modo che il demone amuled venga avviato al boot del PC. Lanciamo il comando "sudo nano /etc/default/". Nella riga AMULED_USER inseriamo il nome dell'utente che deve eseguire amuled all'avvio della macchina: è l'utente con il quale abbiamo creato la directory di configurazione di amule; se l'utente è mario, ad esempio, la riga diventa 'AMULED_USER="mario"'. Poi salviamo il file e chiudiamo l'editor.

:: Colleghiamoci ad amuleweb

Avviamo il demone con il comando "amuled -f" e, quindi, il web server con "amuleweb -q &". Adesso non rimane che connetterci all'interfaccia web dal PC locale: lanciamo un qualsiasi web browser e nella barra degli indirizzi inseriamo "http://localhost:65535/". Nella schermata che appare, sotto la scritta "Enter your password here" digitiamo la password per accedere al web server (è quella indicata nella riga AdminPassword del file remote.conf), questa volta inserendola in chiaro invece che nella forma di hash md5. Dopo aver digitato la password, verremo accolti dall'interfaccia web vera e propria, nella quale potremo gestire gli scaricamenti e le ricerche nelle reti P2P. Per accedere ad amuleweb da una postazione remota, quindi, inseriamo in un browser l'indirizzo IP della macchina su cui è attivo il web server, seguito dalla porta 65535 (Figura 4).